MAANPUOLUSTUSKORKEAKOULU

IMBUING AIRBORNE ELECTRONIC WARFARE SELF-PROTECTION – POSSIBILITIES TO DISGUISE

Master's thesis
1st Lieutenant
Jussi Sippola
SM3
Military technology
April 2014

Kurssi Sotatieteiden maisterikurssi 3	Linja Maasotalinja
Tekijä Yliluutnantti Jussi Sippola	
Opinnäytetyön nimi IMBUING AIRBORNE ELECTRONIC WARFARE SELF-PROTECTION – POSSIBILITIES TO DISGUISE	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka Maanpuolustuskorkeakoulun kurssikirjasto
Aika Huhtikuu 2014	**Tekstisivuja** 63 **Liitesivuja** 0

TIIVISTELMÄ

Tutkielman nimi käännettynä suomeksi on Lentokoneiden omasuojajärjestelmien kyllästäminen – mahdollisuuksia kätkeytymiseen. Siinä keskitytään etsimään aktiivisia, ilmauhkaa kohti säteileviä keinoja ilmahyökkääjän, lentokoneen tai helikopterin, omasuojajärjestelmän harhauttamiseksi. Järjestelmät pyrkivät varoittamaan lentäjää laser- ja tutkasäteilyhavainnoista sekä ohjuksen laukaisusta ja lähestymisestä. Omasuojajärjestelmiin kuuluviin vastakeinoihin tutkimus ei keskity. Tavoitteena harhauttamisella on ilmapuolustuksen todellisen määrän ja sijainnin suojaaminen. Epätietoisuus voi saada lentäjän tekemään vääriä johtopäätöksiä. Työ ei fokusoi harhauttamisen taktiseen kehykseen työn kannalta tarpeellista määrää enempää. Tietosuojasyistä tutkimus ei käsittele käytössä olevien omasuojajärjestelmien operatiivisia ominaisuuksia vaan käsittelee teoriaa niiden taustalla.

Tutkimus tehtiin käyttäen taustatutkimukselle enemmän tyypillistä kirjallisuustutkimusta. Jo tutkimuksen alkuvaiheessa oli oletettavaa, että elektronisiin sensoreihin perustuvaa omasuojajärjestelmää pystytään harhauttamaan. Systeemianalysoinnilla pyrittiin löytämään vastauksia tähän olettamukseen. Omasuojajärjestelmästä muodostettiin jo tutkimuksen varhaisessa vaiheessa malli. Tieteellistä kirjallisuutta omasuojajärjestelmistä on olemassa jonkin verran, ja niistä löydettyä tietoa omasuojajärjestelmien ominaisuuksista ja sensoreista yhdistettiin malliin niin, että siitä saatiin mahdollisimman tarkka systeemin kuvaus todellisesta omasuojajärjestelmästä. Analyysin tavoitteena oli löytää niitä kriteereitä, joilla omasuojajärjestelmä saataisiin kohtuullisen tehokkaasti uskomaan harhautusta oikeaksi hälytykseksi.

Ohjuksen laukaisusta varoittava sensori perustuu ohjuksen moottorin muodostaman pilven lämpösäteilyyn. Säteily kuitenkin muuttuu lennon eri vaiheissa, mikä tuottaa haasteita järjestelmälle. Millimetrialueen tutkan käyttö varoittimen sensorina on myös yksi vaihtoehto. Laser-varoittimet toimivat koko sillä taajuusalueella, mitä sotilaskäytössä tulenjohtamiseen ja ohjusten ohjaamiseen käytetään. Tutkavaroittimen tutkimus on vielä kesken.

Löydettyjä tuloksia analysoimalla tulen tässä vaiheessa hieman ristiriitaisiin tuloksiin. Lämpösäteilyn käytön suurin haaste on sen eteneminen ilmakehässä. Varoittimen tavoitekaan ei ole toimia kymmentä kilometriä pidemmälle. Yksi mahdollinen ratkaisu on suunnitella ja toteuttaa raketti, jonka tuottaa lämpösäteilyä kuten tietty puolustavan joukon käytössä oleva ohjus. Jos koneessa on kuitenkin myös millimetrialueen tutka tukemassa varoitusjärjestelmää, hankaloituu rakettiharhautus merkittävästi, koska sen pitäisi oletettavasti olla lentokoneen kanssa melko tarkasti kohtaavalla reitillä. Laser-varoitin on ilmeisesti herkin järjestelmistä, koska se voi tietyissä olosuhteissa ja varsinkin matalalla lentokorkeudella aiheuttaa paljon vääriä hälytyksiä ilman tarkoituksellista harhauttamista. Laserin käyttö yhdistettynä raketin laukaisuun saattaisi tuottaa halutun tuloksen. Tutkavaroittimen harhautus onnistuu, jos valelaitteen signaali on uskottavan tarkka.

AVAINSANAT
lentokone, helikopteri, omasuojajärjestelmä, laser, infrapuna, ultravioletti, tutka, sensori, harhauttaminen, suoja, elektroninen sodankäynti, elektroninen suoja, elektroninen tiedustelu

CONTENTS

1 INTRODUCTION 1

1.1 Research task 2
1.2 Concepts, Points of view and Exclusion 4
1.3 Theoretical Context 7
1.4 Methods 9

2 THREATS SYSTEMS 11

2.1 Threat systems 11
2.1.1 Overview 11
2.1.2 Non-terminal threat systems 12
2.1.3 Terminal threats 13
2.2 Threat technology 17
2.2.1 Overview 17
2.2.2 EO-sensors 18
2.2.3 RF sensors 20
2.3 Discussion 22

3 RECEIVER SYSTEMS OF EWSP 24

3.1 The purpose of EWSP 24
3.2 Missile warning receivers – Taking Advance of the Infrared and Ultraviolet bands for Detecting Approaching Missiles 25
3.2.1 Features of missile warning systems and measures of effectiveness 27
3.2.2 Observables – what the MWR is looking out for 30
3.2.3 Discussion of MWR systems 34
3.3 Laser warning receivers 35
3.3.1 LWR systems and measures of effectiveness 35
3.3.2 LWR observables 38
3.3.3 Discussion on the laser warning system 41
3.4 Radar warning receivers 42
3.4.1 Radar warning receiver systems and measures of effectiveness 43
3.4.2 Active electronic countermeasures against radar 52

3.4.3 RWRs' observables 54
3.4.4 Discussion of radar warning receivers 56
3.5 Discussion of warning systems 57

4 ANALYSIS OF DECEPTION 59

5 CONCLUSION 63

5.1 Evaluation of the results 63
5.2 Evaluation of the scientific contribution 63
5.3 Suggestions of topics for future researches 63

REFERENCES 1

SYMBOLS AND ABBREVATIONS

Symbol / Abbreviation	*Nomenclature*	*Units*
AC	Alternating Current	
A/D	Analog-to-Digital Converter	
AOA	Angle-Of-Arrival	
ARM	Anti-Radar (/Radiation) Missile	
CPU	Central Processing Unit	
CVR	Crystal Video Receiver	
CW	Continuous Wave	
D/A	Digital-to-Analog Converter	
DC	Direct Current	
DR	Dynamic Range	
DSB	Double Sideband	
DSP	Digital Signal Processor	
ECCM	Electronic Counter-Counter Measure	
ECM	Electronic Counter Measure	
EM	Electromagnetic	
EMI	Electromagnetic Interference	
EMS	Electromagnetic Spectre	
ESM	Electronic Warfare Support Measures	
EW	Electronic Warfare	
EWSP	Electronic Warfare Self-Protection (system)	
FAR	False Alarm Rate	
FCR	Fire Control Radar	
FM	Frequency Modulation	
I	Intensity	W/sr (Wsr^{-1})
IF	Intermediate Frequency	

IFM	Instantaneous Frequency Measurement
LBR	Laser Beam Rider (missile)
LO	Local Oscillator
LRF	Laser Range Finder
LWR	Laser Warning Receiver
MDS	Minimum Detectable Signal
MOE	Measure Of Effectiveness
MWR	Missile Warning Receiver
RWR	Radar Warning Receiver
sr	steradian, SI-unit of solid angle
TOA	Time of Arrival
VCO	Voltage Controlled Oscillator

IMBUING AIR-THREAT – DISGUISE AS A PLOY TO DISTRACT AIRCRAFTS

1 INTRODUCTION

Today's theatre of war has changed radically from the times of Sun Tzu, nevertheless, many things remain the same. Strategy – the art of winning a war – has clearly an equal meaning historically and today, but the means to attain it have drastically changed. In the field of tactics, we have come probably even closer to the means of Sun Tzu; battles in counterterrorism or counterinsurgency missions are nearly entirely deception and fraud from the hiding party's point of view.

The main intent of my research is to prove that historical operations like Operation Overlord — the landing and occupation of Normandy — and many others would not be possible in today's battlefield the way they were accomplished historically. Radars would have given an early warning of the enemy's manoeuvers far at sea for the defender in Normandy.

The biggest difference between war-machines is in, frankly, the sensors; including air, land and naval vehicles. The implementation of armour and armament of a tank has not changed significantly in the past decades. What has changed is the thickness and hardness of the armour and therefore the continuously developed armour penetrating munitions which has longer range. The warships have transformed into large missile carriers, and missiles most specific parts are the high-tech sensors: infrared sensors, radars, GPS-receivers etc. And the real focus in this research, the warplanes and helicopters, have gained more and more speed and manoeuvrability by the development of the jet-engines, aerodynamics and fuselage design and construct. However, the most lethal thing about them as well is their weaponry — precise air-to-air and air-to-ground missiles which apply the different uses of sensors; not to mention the sensors the aircraft itself is carrying with it on its radars, FLIRs or missile warning systems.

Contemporary war machines carry multiple sensors covering a great deal of the electromagnetic spectre. It is nearly impossible to stay undetected on the ground though forces would be entrenched and camouflaged. At some point they will be noticed and usually this is eventually when a shot is fired by the ground troops or a signal sent from a radio transmitter or a radar. My key topic and point of interest in this research are the electronic warfare self-protection systems EWSP the warplanes and helicopters are carrying (in some sources also known as MWS = missile warning system or MAW = missile approach warning). The EWSP is used to detect and warn the pilot of the radiation of a laser or an air defence radar, or of an incoming missile which it has noticed. They are designed to warn the pilot, deploy the countermeasures accompanied with counter manoeuvres to prevent the missile hitting the plane. These missile warning systems sense different radiations from the environment. They detect these radiations if present, make calculations of the detection, try to identify the threat, and give the pilot a warning. Simultaneously they can even deploy the countermeasures, flares or chaff, if set to an automatic mode.

At this point well-designed and managed disguise-attacks come into picture which will be my main task, as described later. With the help of multiple simultaneous false attacks it must be considerably more difficult for the enemy to define real attacks from decoys, which in turn makes actions against real threat a lot more fragmentary and difficult. In addition it must be very frustrating to the pilot to engage in the avoiding manoeuvres and wasting the countermeasures if warning signals are flashing all the way. This brings a sort of small-scale PSYOP-dimension to the means of distractions and his concentration on the mission is greatly disturbed. I cannot resist to quote Colonel Andy Birdy from USARMY, who said during the operation Uphold Democracy in Haiti

> *"Psychological operations...have proven to be indispensable...it allowed us to apply a type of power without necessarily having to shoot bullets.*[1] *"*

That said, before going any further to the research tasks and delimiting them, any greater value for PSYOPS than is needed in a technical research is not given.

1.1 Research task

The research task I have defined for this paper is straight forward: how to bring the surprise element back in the art of air defence warfare with the assistance of active electronic warfare. In The Air Force Doctrine Document 2-5.1 actions like these are named electronic deception

and they are defined as "[deception] Utilizes the electromagnetic spectrum to confuse or mislead an adversary.[2]" This thesis will not answer all the questions about the surprise-element on the battlefield, not even from the point-of-view of the ground based air-defence. In other words, the main research problem in my thesis is,

- what are the best possibilities to succeed in deceiving the airborne electronic warfare self-protection systems?

This research is not from any particular troop's point-of-view, but as general as it can be. Threats of aircraft, countermeasures against them, and deceptive actions searching possibilities to imbue them are the most significant subjects in the text. Some air defence troops on the battlefield fighting as part of a virtual, non-specific army troops are used as examples a few times.

My supplementary tasks are:

- What is the electronic warfare related threat to a combat aircraft, and what kind of transmits and emissions it sends?
- Which bands of electromagnetic spectre are covered with the different sensors of EWSP system?
- What are the observables of the receivers, and how do they discriminate a real threat from a false alarm?

Other pressing questions after the conclusions made to the questions above are:

- What type of machines could do the decoy's job and what kind of requirements for these machines should be given?
- Does industrial devices already exist that could complete the mission without being deciphered by the enemy?

Determination of the bands the different sensors of a warplane are using will be practically solved rather simply. All that is needed is a few good sources of material considering the MWS in general and gathering the information about the basic principles of the MWS and what sectors of the EM-spectre they are using. After that shall be introduced more specific information about the state-of-the-art sensors, including their abilities and limitations. In the

end should be possible to claim how the EWSP system and the pilot could not be able to recognize the real attack from a false alarm.

Clearly a challenge will be to find accurate data from up-to-date MWS-applications which are in operative use because of classifications. In the section where I'm trying to meet the task of "how the MWSs discriminate the real threat from a false one" I need to make drastic conclusions from the knowledge gathered from non-specific literature and other sources considering computer algorithms and electromagnetic radiation features.

The last two problems to-be-solved follow in the conclusions made from the first chapters. This will be mainly requirements for a decoy to survive the cut: not to be recognized as a decoy. The industrial part of this paper shall remain a narrow sweep of what components or ready systems would the markets already have.

1.2 Concepts, Points of view and Exclusion

"*Concepts* are the constituents of thoughts. Consequently, they are crucial to such psychological processes as categorization, inference, memory, learning, and decision-making. This much is relatively uncontroversial."[3] Still, the nature of concepts varies depending on what is the philosophy behind it and thus concepts have been the subject of much debate. Concepts are either mental representations – psychological entities – of a larger subject or just simply abilities. The third philosophy is so called Frengean Sense, which --

From the three variations above I have come to conclusion to think the concept of my paper as a mental representation of my subject being examined. I have touched my concepts briefly in earlier chapters and will have a more specific glance at them here. The concept of this research is as follows:

If it is presumed, and so it should, that a target on the ground will be, at least by means of EW, found by air war machine over hostile ground and especially while on a DEAD/SEAD mission (destruction/suppression of enemy air defence), albeit they would be well camouflaged and hid, the probability of finding the real targets will be made somewhat more difficult if there would be even more of targets found than real targets – the real threats for attack-planes or helicopters – exist. (Figure 1)

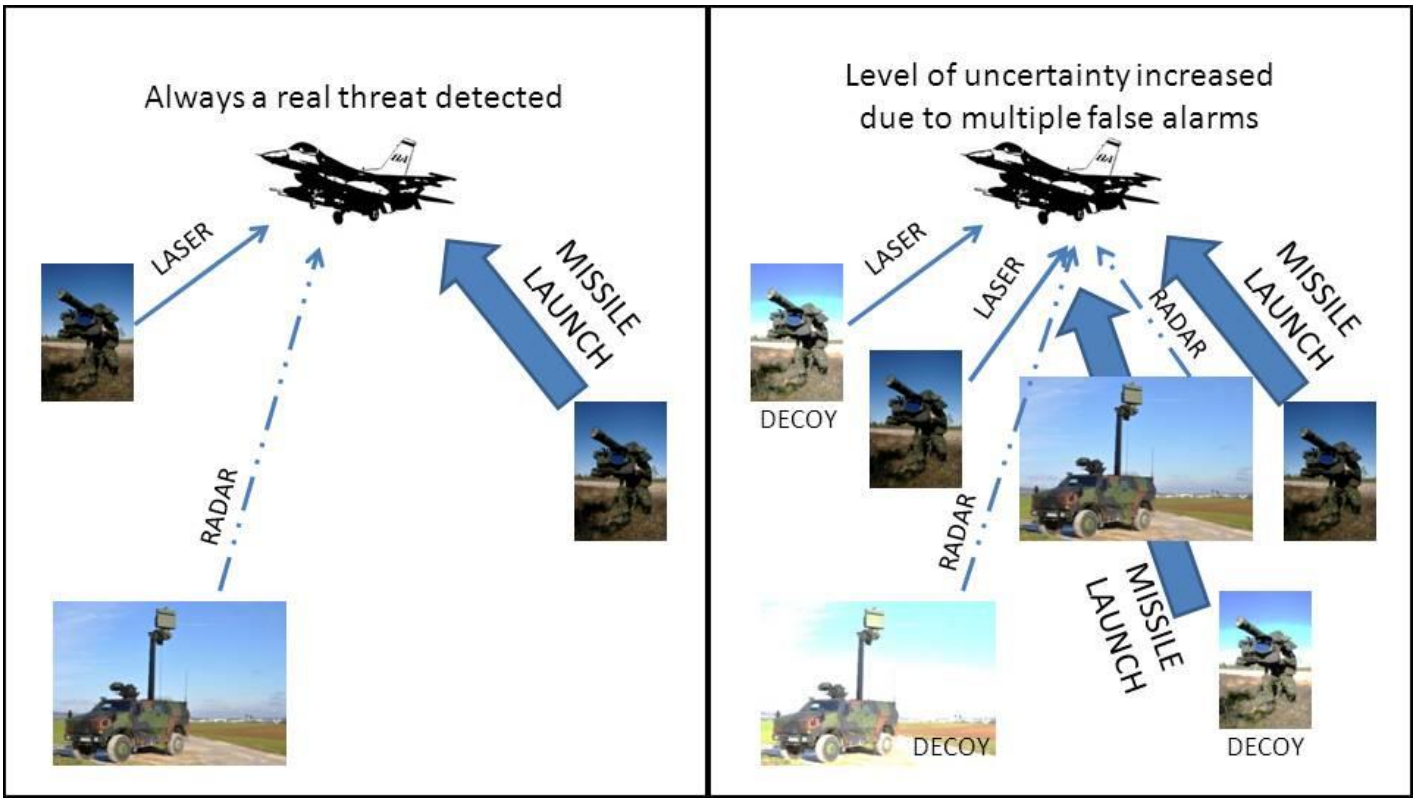


Figure 1: The concept: for the aircraft it is severely more difficult to certainly know when to start the countermeasures if the MWS is warning repeatedly. This gives the defender on the ground more cover for its actions.

Means of detecting these threats of an attack plane are many. Electronic reconnaissance is done with platforms solely built for this purpose or by electronic devices aboard the attack-plane. I will concentrate more on the attack-planes, but reconnaissance planes are potentially equally affected by the ploy. A target can be detected from the emission of radar or laser, or from the launch of missile, which emits measurably and quite typically in the regions of visual light, infra-red and ultraviolet regions, and can thus be used for the detection. [Figure 2]

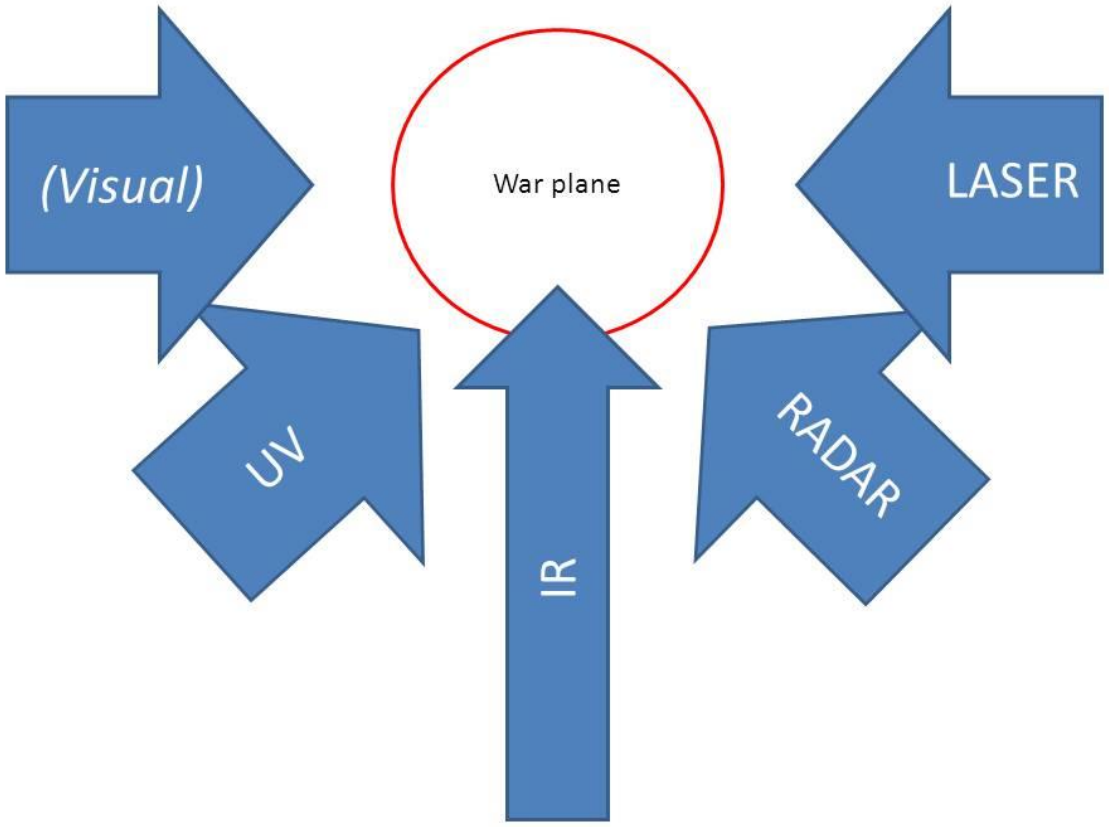


Figure 2: The means of an attack-plane to detect threats on ground.

When it's made difficult for the pilot to determine when the threat is real, the defender of the ground has significantly increased its probability to survive. This could occur other consequences, as well: the aircrew could turn around, concentrate to decoy and miss the real threat, or even firing towards the decoy. When the MWS indicates Calculations for the probability are presented later.

The line between active and passive decoy in my paper is drawn between either the decoy transmits radiation of any sort by purpose, and which is the key to deception of it, or not. Dummy rockets, which come to picture when trying to alert the sensors seeking for missile launch, are in the twilight zone. They are not electronic transmitters, but their main purpose is to create infra-red and ultra-violet radiation plausibly. My point of view is strictly in the active disguise. I will not concentrate in passive decoys, which are a topic for a whole other paper.

Open Source Intelligence (OSINT) will be my one of my methods in the search of data and usage of sensors. Practically, this means the usage of IHS Jane's database and usage of many

different military magazines. Using the internet as source has it place when finding first clues about new subjects.

As the paper progresses to its Analyse chapter, I will present different solutions for making these disguise-attacks. One preliminary assumption I have beforehand: I believe large enough rockets are possible for this application. I have found out that in the UK they are in use for testing purposes. Despite being a very interesting matter nothing came up with reasonable amount of search.

1.3 Theoretical Context

Theoretical context of this paper is difficult to outline. In the centre are the electronic warfare self-protection systems that are designed to warn the flight-crew of helicopter or aircraft against a variety of threats in the battlefield that could occur during a mission. Laser beam, radar radiation, and a launch of a surface-to-air missile are the ones to be noticed with advantage taken from the electromagnetic spectre. They are the threats that are extremely lethal, or their existence in the moment could lead to hazardous incidents later. More time to react is acquired by noticing the presence of the threat earlier. The three indications of threats mentioned above are the easiest ones to pick from noise, and thus most useful from the aircrafts point of view. And the big picture of electronic warfare (EW) and its operational functions [4] come into question when talking about electromagnetic spectre, including the electronic attack (EA), the electronic protection (EP) and the electronic support (ES) with the signals intelligence and their interactions as visualized by Alm in Figure 3. Electronic deception as a greater entirety of military deception is, however, an equivalent action on the list of command and control (C2) warfare actions:

- Operation security (OPSEC),
- EW,
- Psychological operations (PSYOPS),
- Military deception, and
- Physical destruction [5].

PSYOPS was noticed briefly in the first chapter, but deserves no more attention later, because of it not including into the theoretical context or research task. It is an additional advantage, in size of single pilot or squadron, that might occur, and has its place as part of an more psychological research.

Missile warning systems are systems-of-systems; they are more than the sum of their subsystems abilities. Sensors and data processing units, which calculate the data coming from the sensors, are the subsystems going to have most attention in this paper. The sensors acquire the data of signals directed to the target plane, or at least are visible to it; the data processing units (DPU) most value is from its ability to define the real threat-demonstrative signals from false alarms. Getting deep into the DPU's methods could become overwhelming, and I might have to leave it to minor interest. MWS's operative capabilities are commercial secrets hard to find accurate data from. All that is possible to do is to model their work by studying the procedures of computer algorithms, and doing strict speculation from them. Other subsystems are not in the centre of interest in my research, and thus will be left to minor focus.

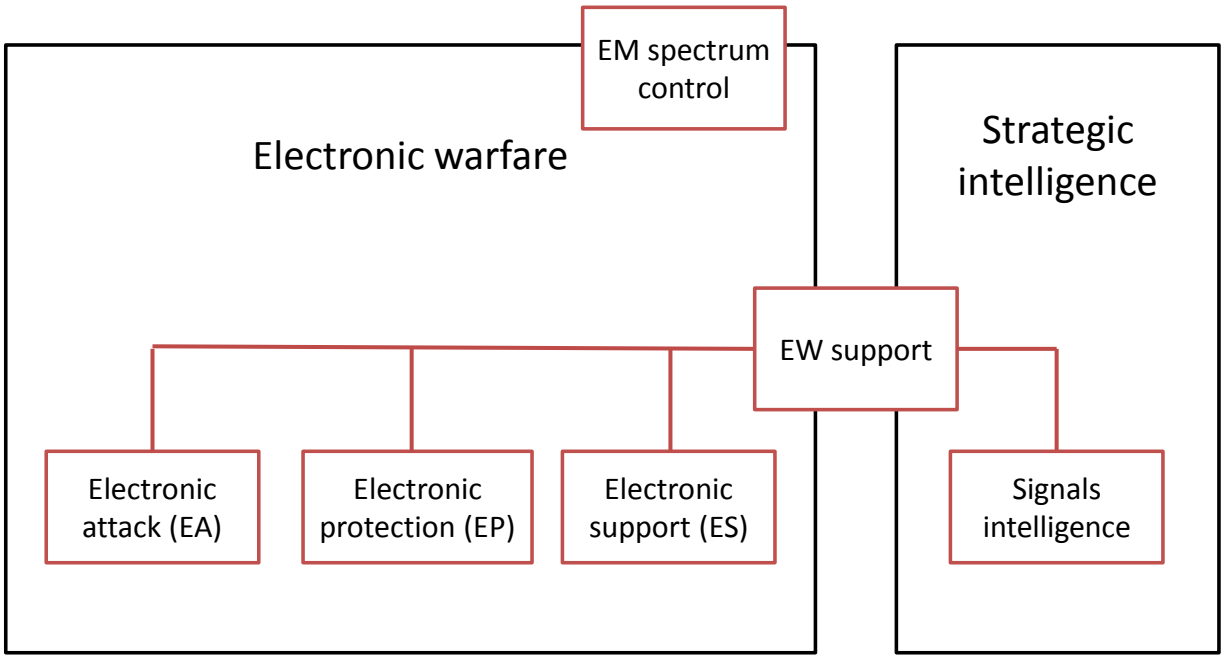


Figure 3: Operational functions in electronic warfare and sectors closely related to EW. [4] In a version of the same functions on De Martinos' book [5] is longer lists under the three headlines of EW, and 'signals intelligence' is under the electronic support. ECM methods, where this paper is aiming to, are in two positions in his diagram. ECM could be thought to belong to either one of them: from this paper's questions' point-of-view is to answer in problems of deception, but the aim behind is to acquire more protection to the land based troop.

To accomplish my research I have to what the threats of aircraft are, and how they are visible to aircrafts' sensors. After presenting these threats it's easier to the researcher, and reader, to understand the methods and meaning of the MWS and requirements of the decoy. The main

task of this research is, in other words, to find the relevant features of the land-based air-defence equipment that could possibly rather easily and plausibly imitated, and thus acquire desired reactions in the aircraft and its crew. The theoretical context from the point-of-view is this paper is shown in Figure 4.

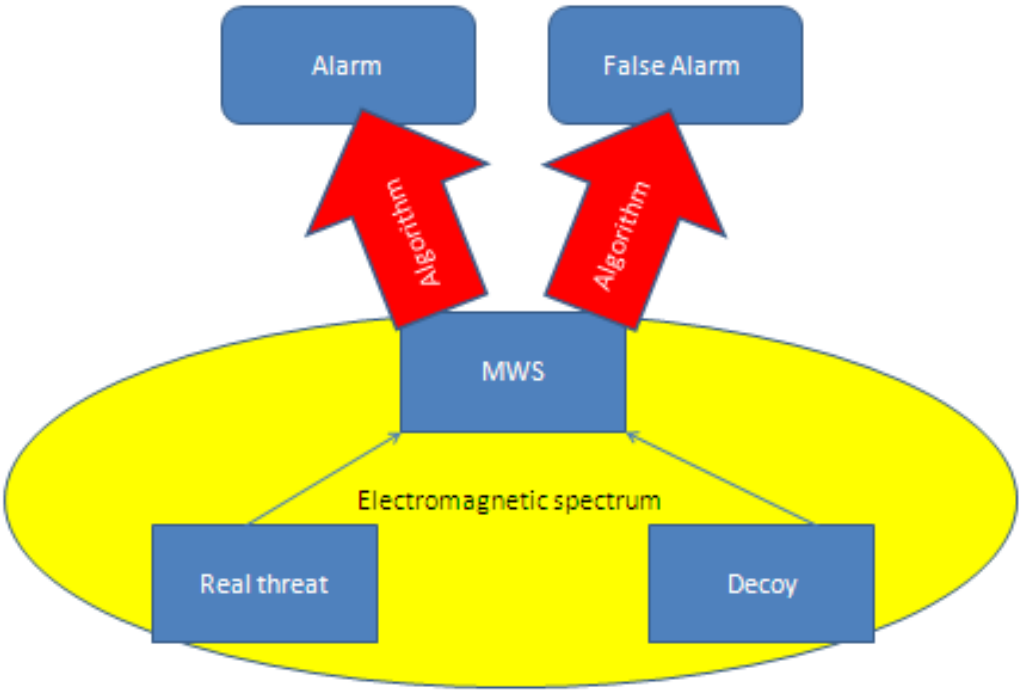


Figure 4: The theoretical context of EW from point-of-view of this research. This sketch was made in the very beginning of the process, and long before deeper knowledge of the subject was evolved in the mind of the researcher. It is not misleadig in any way, but it's little abridged for to be used alone.

1.4 Methods

Doing a theoretical literary research of a pragmatic subject is a difficult task in different levels. Aware and justifiable ontological decision is something different than just a thought. Still mostly they are mere notions without any deeper understanding. Basis of the research must be on solid ground. Doing an academic research always includes some basic presumptions or philosophical commitments. These are facts on which the process of the research is based on. This is true even in a very pragmatic research or when the research aims to work-oriented solutions usable in everyday life. It applies even though the theoretical basis would be some-

what shallow, just like it was in the beginning of this paper. [7] When this research had begun about 18 months earlier than it was finally ready these presumptions and predictions seemed very distant. This research is built logically from the basis to the answers of the research questions. Many things are taken granted in everyday life – and sometimes in academic research, as well. Taking reader's knowledge as granted has been avoided, as is a good academic custom [8]. Still some background in the basics of military tactics and especially electronic warfare might come handy.

This paper has been made as a literature research [9]. Some elements of system analysis has considered. All the sources are public, yet not everyone in the reach of all readers. Most data from the sources is collected in the third chapter, which is presenting the technology of warning systems, and physics involved with them. Answers were found with deductive analysis: inferences were made from the information gathered in the two data chapters ahead of the analysis when the research was reaching towards the completion of the main tasks. In the line between qualitative and quantitative research this falls very close to the qualitative end. Final discussion reconciles the entity.

2 THREATS SYSTEMS

2.1 Threat systems

2.1.1 Overview

According to STANAG 2999 [11], the threats to helicopters in land operations are air defense weapons (i.e. small arms, anti-aircraft artillery, and air defense guided missiles), tank main armament, anti-tank guided missiles, field artillery, tactical aircraft, armed helicopters, EW, and NBC warfare. [12] Robert E. Ball [13] has made a substantially more complete list of the threats for helicopters in battlefield, shown in Figure 5. Though the figure is made of threats concerning the helicopters I have no reason why not to count the same threats have an impact on larger group of different aircraft. I have dropped out some insignificant threats considering this paper.

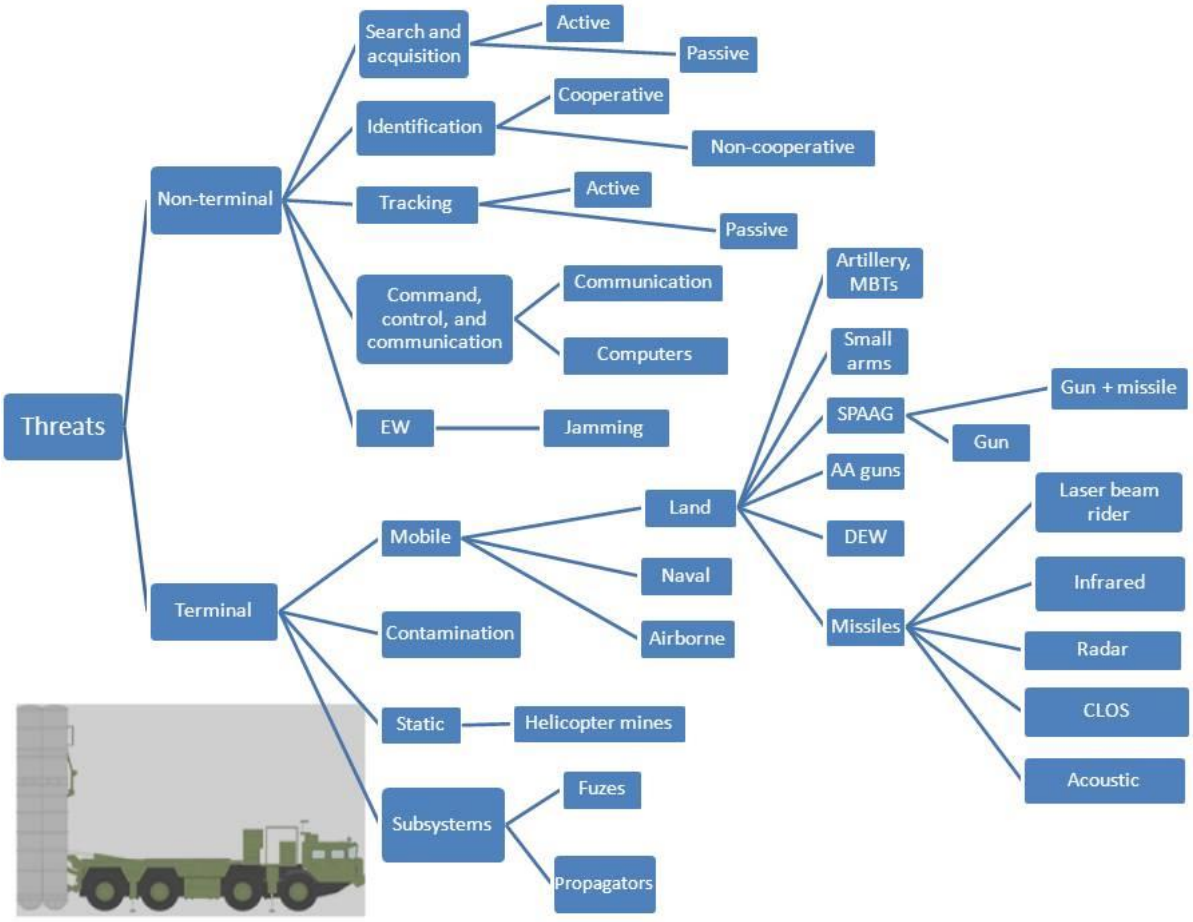


Figure 5: Helicopter threat types, via Heikell [11]. Legend: MBT = Main Battle Tank, SPAAG = Self Propelled Anti-Aircraft Gun, DEW = , CLOS = Command Line-of-sight.

2.1.2 Non-terminal threat systems

Non-terminal threat systems augment the effectiveness of terminal weapon systems. They provide acquisition, identification and tracking of the target and distribute this information to weapon platforms. They can also lower the helicopter's efficiency through means of electronic warfare. Thus, non-terminal threat system does not constitute the aircraft a threat *per se*. These threads, more specific listing in table, are very significant considering my research and will acquire more specific consideration later in the paper. A summarization of non-terminal threats is made in Table 1.[11]

Table 1: Summary of most important non-terminal threats to helicopters (cf. Figure XX) via Heikell. [11] Heikell was interested in his paper solely on the threats of helicopters in the battlefield, which is rather easy to decide from his notation on his work, and especially this table. However, many of these non-terminal threats can be conceived on aircraft, as well.

System task	*Systems/methods*	*Features*
Search and acquisition	Active uni- or multistate radar systems, passive SIGINT and ESM systems, IRST and other EO systems, acoustic helicopter detectors, human observation. Airborne systems increasingly used for enhanced coverage	Radar frequencies from VHF to X-band(IEEE std), multitude of modulations and search schemes, transmit powers from sub-Watt to MWs. ESM and SIGINT systems covering HF through Ka-vand, with sensitivities below -100dBm. EO systems covering the visual 12 µm band. Aural detectors sensitive in the lower frequency range of helicopter rotor noise.
Identification	Cooperative through active IFF systems; non-cooperative by radar identification, EO systems and/or visual observation or identification of emissions by ESM systems.	Encrypted IFF interrogations and responds at designated frequencies. Non-cooperative systems through signal processing in search / acquisition sensors, supported by emitter libraries. Radar ID of turbine and rotor modulations or target glint pattern. EO ID through pattern recognition. Hybrid ID methods for enhanced effectiveness.

Tracking	Software tracking functions of search radars and EO sensors. Combined search and track with ESA and track mode of airborne radars. Dedicated track (fire control) by mechanically steered antennas. Triangulations by SIGINT or ESM for rough track. Track by human observation.	Track function in traditional search radar as a display feature; in EO sensors tracking is by signal processing and pattern recognition or human assisted. ESA radars can switch between search and track and have no fixed spatial scheme; present fighter aircraft radars mechanically lock their antenna for tracking, as does dedicated fire control radars. Monopulse tracking dominates modern radars. Triangulation with cooperating or airborne systems.
C3	Mobile ground/air/space communication systems; not a point-of-interest of this paper.	Radio or wire communications.
EW	Electronic countermeasures against helicopter radar and communication systems.	Saturation and / or deceptive jamming to degrade helicopter's effectiveness as a combat asset.

2.1.3 Terminal threats

As is shown in the Figure 5, terminal threats, threats that try to have an terminal impact on airborne craft can be subcategorized in static and mobile systems. In here the terms mobile and static could be a little misleading. Basically all weapon systems are counted as mobile systems though they are very static when operating. If a static object is solid it could end up being a lethal threat to helicopters and other aircraft flying on low altitudes: smokestacks, hills, communication link antennas, etc. Relevant battlefield intelligence with attention to terrain are basic precautions needed to pilot a helicopter through safely. Helicopter mines are the most noticeable tactical static weapon. Other aircraft don't have threats as mines to threaten their mission anymore, but historically barrage balloons used to act as such. They have been obsolete since the Second World War. [11]

The threats falling under headline "Mobile" are various, hence not all remarkable according to the research tasks of my thesis. Such are: Small arms and RPGs; artillery and MBTs; and most from the groups anti-aircraft guns and SPAAG. In the same class, mobile, are all of the naval and airborne threats, and I will not attend them any interest, as well. [11]

2.1.3.1 Anti-aircraft guns and SPAAG

In my concept-chapter I introduced my idea of producing radar-like radiation as one of the methods of imbuing the aircraft. When speaking of the threats of an aircraft one of the very dangerous ones is the sub-group 'radar-guided guns'. When combining the precision of a tracking radar to the fire-rate and accuracy to close-distance of a gun, you achieve a system of high lethality to targets flying low. Atop them, AA guns have better multi-target capability than missiles and with guns it's easier to sustain a non-penetrable barrage around a point target to protect it. [11]

SPAAG vehicles often carry both search and track radars, and the gun is gyro stabilized for firing in the move. A new variation of SPAAGs is to add short-range missiles on them, which increases their range and the number of targets that can be engaged. [11] Table 2 and Table 3 show details of some examples of AA guns and SPAAG systems.

The aspect of radar guided AA guns from the deceptive point-of-view is revisited in the analyze chapter.

Table 2: Specifications for some AA gun systems. via Heikell.[11] Legend: F/T = Fragment - timed, AP/T = Armor piercing - timed, m(v) = meter vertical.

	S-60	*Bofors L/70*	*Skyshield 35 AHEAD*
Country of origin	Russia	Sweden	Switzerland
Caliber	57 mm	40 mm	35 mm
Muzzle velosity	1000 m/s	1000+ m/s	--
FCS	Radar/Optica	Radar/Optica	Remote only
Rate of fire (/barrel)	105-120 rds/min	260 rds/min	1000 rds/min
Elevation/Depression	+87°/-2°	+90°/-4°	--
Traverse	360°	360°	--
Drive type	Servo/Manual	Electrohydaulic	Electrical
Effective range	4000-6000 m(v)	3000-4000m	--
Ammuntion	F/T, AP/T	Numerous	AHEAD

Comment	Produced from 1950 to 1957	Entered service in 1951	Ready for pro-duction

Table 3: Specifications of some IR guided MANPADSs, via Heikell.[11]

	Gepard	*2S6M Tunguska*	*LvKV-90*
Country of origin	International	Russia	Sweden
Caliber	2 * 35 mm	2 * 30 mm	40 mm
Missiles	--	9M311 (SA-19)	No
Sensors	S/T-rdr, EO, LRF	S/T-rdr, EO, opti-cal	T-rdr, EO, optical, LRF
Gun / Missile range	3000 m	4000/8000 m	--
Max. Missile speed	--	900 m/s	--
IFF	Yes	Yes (1RL138)	--
Comment	Missile upgrade developed		CV-90 chassis
Legend: S/T-rdr = Search / Track radar, T-rdr = Track radar.			

2.1.3.2 Missiles

Missiles are a threat to helicopters, if it can operate at low altitudes, but for a warplane they are a threat almost invariably. MANPAD missiles alone have been built in so big numbers that they will be encountered in any scenario throughout the world. Table xx shows details of some common IR guided MANPAD missiler; LBR and CLOS missiles are in Table 4.

Table 4: Specifications of some IR guided MANPADSs, via Heikell. [11] Legend: FM = Frequency modulation

	Mistral 1	*Igla*	*FIM-92B/C Stinger*
Country of origin	Europe	Russia	USA
Min/Max slant range	300/6 000 m	500/5200 m	200/4800 m
Min/Max eff. Alti-tude	5/3000 m	10/3500 m	>0/3800 m
Seeker	2-4/3,5-5 µm	1,5-2,5/3-5 µm FM tracking	0,3-0,4/3,5-5 µm
Preparation time	--	6 s	--
Speed	M2,5 max	M2+	M2.2
Burn-out/self-destruct	2,5 s/14 s	--	--
Warhead	1 kg HE	1,27 kg HE	1 kg HE
Fuze	Impact & laser proximity	Impact/Delay	Time delay impact
Comment	ECCM through push-up /-down	9K38 (SA-18), FM seeker	Produced also in Europe

Medium and long-range surface-to-air missile systems provide a threat to helicopters when flying at elevated heights, and other aircraft usually constantly in the battlefield. They could make a threat to helicopters at low altitudes, if the mask from terrain is scarce. Medium and long-range missile system demonstrated in Table 5.

Table 5: Specification of some medium and long-range surface-to-air missile systems, via Heikell.[11] Legend: HEF = high-explosive fragmentation, HEB/F = high-explosive blast/fragmentation, S/A = semi-active, SC = shaped charge, TVM = track via missile.

	ASRAD-R	*Crotale NG*	*S-400*	*Patriot*
Country of origin	Germany, Sweden	France	Russia	USA
Max effective range	8000 m	11000 m	120-400 km	70 km
Min/Max eff. Altitude	<0/5000 m	--/6000 m	185 km	60/>24000 m
Sensors	X-band 8.8-9.3 GHz,24 frequencies, FLIR, TV, LRF	102-2,4 GHz PD S-rdr, 16,0-16,4 GHz monopulse PD T-rdr	"panoramic radar and multifunction radar",	C-band ESA S/T-rdr and up-/down-links
Guidance	LBR	Radio command	Inertial with S/A terminal homing	S/A TVM
Speed	M2	--	M12	M5
Warhead	SC/HEF	13 kg HEF	--	91 kg HEB/F
Fuze	Impact & laser proximity	Impact & proximity	--	Ka-band proximity
Comment	In use in Finland	In use in Finland		PAC-1

2.2 Threat technology

2.2.1 Overview

A more detailed analysis of the technologies used by threats of an aircraft is needed before the countermeasures can be presented. Figure 6 summarizes these technologies. This chapter will shortly describe how the missiles find their way to their target. The technologies used in guidance units of different missiles will be presented. Concentration is in methods and technologies which are not silent in the matter of EMS, but which radiate so that the EWSP could detect the use of the threat. This means practically laser beam-rider technology. Other big topic is the principals of radar technology. These both subjects, and radars, make the biggest signif-

icance of this whole paper from the ploy's point-of-view. It is rather difficult to imitate something electronically if the example doesn't radiate either.

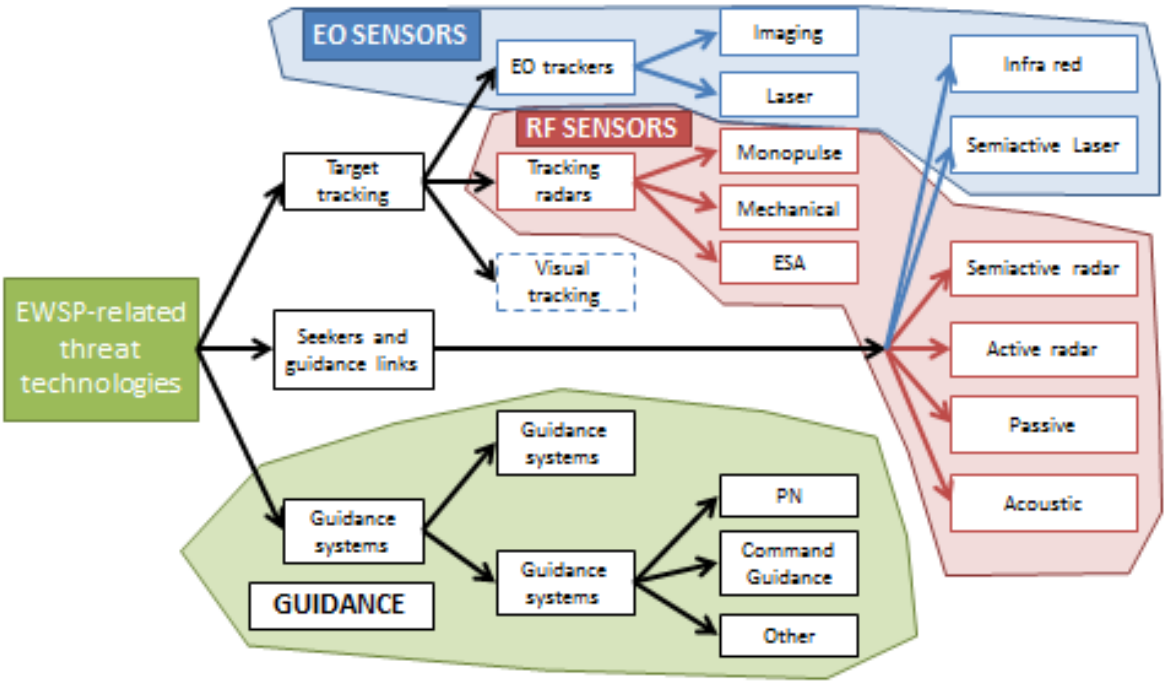


Figure 6: Summary of threat technologies of importance to airborne EWSP-systems.[11] The sensors transmitting are not quite informatively displayed in the diagram, but briefly: EO sensors don't emit or transmit at all; tracking radars, semiactive radars (homing), and active radars (homing) are transmitting, but the rest of the RF sensors are silent in this matter; guidance systems here mean truly the system that transmit in the EMS to hit their target, so they belong to the transmitting pool of technologies.

2.2.2 EO-sensors

2.2.2.1 IR sensors and seeker technology

Imaging technology is a group which consists of low-light television (LLTV) cameras, image intensifiers, and infrared cameras of various types. Naval applications are the main user of LLTV cameras, and short-range systems of the image intensifiers. Both systems are very competent in doing their task but lack interest as subject for this paper for a very evident reason: they don't radiate in any way thus they cannot be placed by a distraction. Other points of views are needed. [11]

Missile warning receivers (MWR) are developed For the purpose of noticing the missile launch. The aircraft cannot be distracted in any other way than building a dummy, and dum-

mies were not in the interest of this research. Possible ploy could be, though, achieved through simulating the missile launch itself. Distracting the missile launch warning is dealt with in later Analyze chapter. [11]

2.2.2.2 Laser technology and guidance

Lasers are part of helicopter threat systems in the form of laser range finders (LRF), semi-active target designators, guidance beams for LBR missiles, and laser fuses. Most significant difference between the LRF and LBR systems is the pulse repetition frequency (PRF) and pulse energy: the LRF uses typically medium-energy, low PRF lasers and LBR-systems use low-energy, high PRF (up to some 10 kHz) devices.[11]

Numerous wavelengths are possible for use in different lasers but only a few are used in practice. For instance, CO_2 lasers operate usually at 10.6 µm in the mid-IR band, but CO_2 lasing has been demonstrated at least for the 8.9–12.4 µm band. The real backbone of military lasers are the Nd:YAG (neodymium-doped yttrium aluminum garnet) lasers at 1.064 µm wavelength, at the near-IR band. [11]

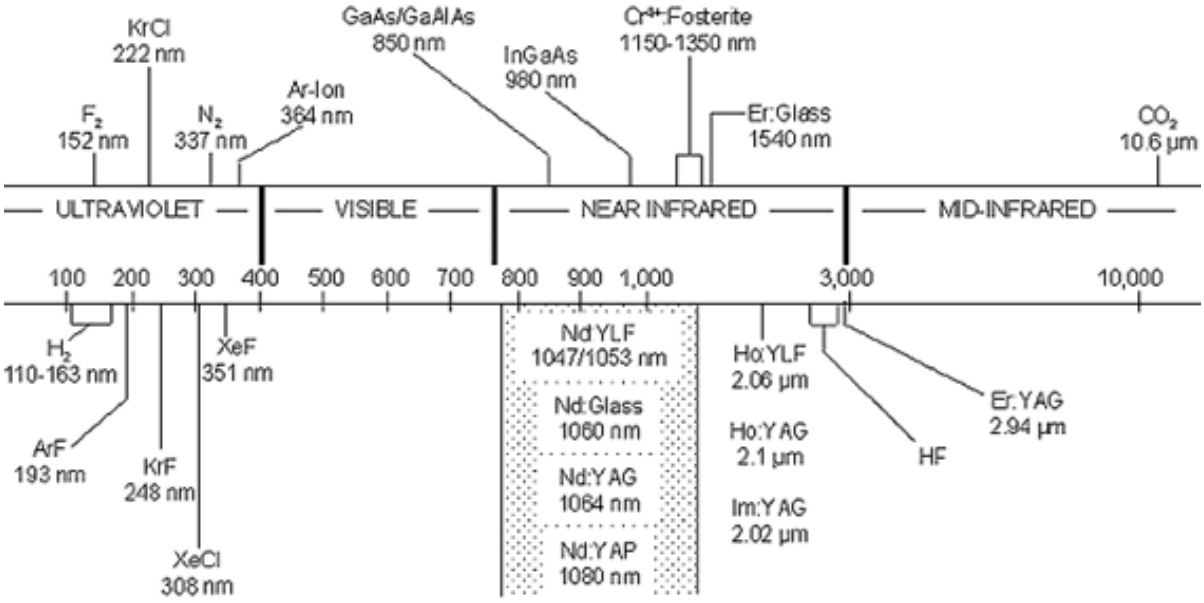


Figure 7: Laser wavelengths of most interest: CO2 at 10.6 µm; Nd:YAG at 1.064 µm;. Other wavelengths are also visible, though not maybe important from the military perspective, of for this research. [14]

LBR missiles laser receiver is in the rear, facing at the behind to the source of the laser beam. The receivers are therefore generally assumed immune to jamming. Hence, the radiation is pointed directly towards the target, which accordingly means it could be easily detected. However, just after the launch the beam has to be broadened, which lowers the beam power density at the target and its sensors, and could cause delay in the detection of the radiation and its source. [11]

2.2.3 RF sensors

Radio frequency sensors can be divided into two main groups from the aircrafts point of view: passive electronic support measure (ESM) and signal intelligence (SIGINT) implements and their sensors, and emitting RF sensors. The passive sensors cannot be detected by the other side, so once again I leave them out of this paper. In addition, emitting sensors are one of the most important subjects in the research, like noted before.

It has been said that "-- every ECM system should be designed to counter the threat to the specific craft to be protected, not every radar in the general area.[15]" This had been brought to usage after the 1973 Yom Kippur where the 2K12 Kub/Kvadrant and the ZSU-23-4 were successful. Western militaries focused for a long time on the emitters of those systems. In Heikell's opinion the notation above is not quite up-to-date anymore. [11] Since 1982 Falkland war, where British aircraft were fighting under the threat of French Exocet missiles, the "western" forces have fought against western military technology. The same had been with Soviet troops in Afghanistan. The "rainbow threat" of almost any possible weapon system is reality in international operations. Only in the national level of small countries the single threat scenario is plausible [11]. The Table 6 below will give a general review of radar parameters of importance to helicopter EWSP, and is quite well broadened to be used with aircraft as well.

Table 6 is also an important source of information to add in the chapter . It is still well justified to keep it here because of it vital information of the radar threats. At the same time it provides excellent summary of the radar RF signal observables, which are more discussed in radar warning receiver chapter.

Table 6: Radar parameter considerations of importance to EWSP and survivability via Heikell. Legend: CPI=coherent processing interval, IBW=instantaneus BW, ICW=intermittent CW, LFM=linear frequency modulation, SLB=sidelobe blanking, SLC=sidelobe cancellation, τ=pulse/code element legth. For more information about matters presented here, refer to chapter 4.4 Radar Warning Receivers.

Parameter	*Importance*	*Parameter range*
Carrier frequency	Single most important parameter for radar identification	The 2-18 GHz band most important to EWSP. Tracking radars increasingly usa Ka-band, and weapon seekers the W-band. Frequencies <2 GHz increasingly cluttered by civil emitters. X-band contains e.g. the bulk of civil navigation radars.
PRF	PRF ranks second most important parameter for radar identification.	PRF from <1 kHz (search radars) to 1 MHz (PD missile seekers). Fixed, staggered, or completely random (in MTI radars).
Pulse width	Third most important parameter for rad identification. Related to BW and PRF.	Pulse lengths from <0.1 µs to >10 µs. Duty cycles from 0.1 %, and up to 50 % for ICW operation. Risk for PW corruption by multipath propagation.
Scan type	Mechanical scan: indicates threat's intension and is a target for deception. ESA antennas complicate the situation.	Circular or sector scan (0.2–2 Hz) for search radars. Intermittent for tracking radars in acquisition phase, and virtually constant when locked. Random looks by ESA radars.
Power	Determines power density at the receiver, which is a main issue to detection.	Transmit powers from <1 W (FMCW) to the MW class (high-power pulsed search radars). EWSP receivers can see any power density depending on the range to the radar.
Bandwidth (BW)	Puts similar requirements on the EWSP receiver.	Pulses shorter than 0.1 µs require >10 MHz IBW. Frequency agility up to 10 % of carrier frequency. (BW ~ 1/τ)
Digital beamforming (DBF)	DBF allows beam nulls to be placed in the direction of a jammer.	True DBF by ESA antenna, pseudo-DBF (SLB/SLC) by added auxiliary antenna(s). Jamming suppression -20–-30 dB, with potential for more.
Polarization	Influences antenna losses and is needed as a jamming parameter.	Any polarization must be expected. Antenna cross polarization (-25 <-40 dB of main polarization direction) is an avenue for jamming.
Coherence	Introduces requirements on jamming coherence.	Depends on victim radar's CPI and stability of its local oscillator.

Coverage	Determines whether a target will be detected or not.	Detection requires that spatial and temporal search conditions are satisfied; frequency domain influences lobe properties and hence the space.

It is obvious that the parameters shown above will show a significant importance in this research. They will be pointed back to in later in the paper, when dealing with the radar warning receivers in chapter 4.4.

2.3 Discussion

Clarifying example of the emissions of the target on the ground, or airborne and at the sea, is in Figure 8, and as it clearly brings out the targets can be visible on ground radiate in two different ways: either they radiate themselves, or reflect radiation coming from other source; background, target illuminating device, sun, et cetera. The reflected radiation is regarded, and, as said before, the interest is in the radiation transmitted, or emitted by the target or the threat on the ground.

For a memory reference, the supplementary task which this chapter was searching answers to was: *What is the electronic warfare related threat to a combat aircraft, and what kind of transmits and emissions it sends?* To answer the question more completely than just with the Figure 8, there is a brief table next to present the most important observables of the targets — or threats, depending on the point of view, here threat more implicit— on the ground.

Table 7. A selection of the transmitted threat signals.

Threat	*… and a selection of its possible observables*
AAA and SPAAG	- laser range-finder - Radar signal (if exists), can be determined as FCR by its “radar locking” and mechanical scan on target. [Table 6]
SAM	- heat propagation of the missile plume, and/or the surface of the skin - RF guidance signals (CLOS, TVM) - radar signals (active/semi-active radar homing, ACLOS) - laser range-finder - laser guidance (LBR)
Radar	[See Table 6]

This chapter gave a very short and not very detailed picture of airplanes' and helicopters' threats on the surface. Due to the more important issues, research questions and priorities of this paper, these are not addressed in this study further. Later chapters will continue, however, the discussion of threats because of separating them completely from the receiver technology is almost impossible. The next section explores the literature of the EWSP receivers, and it will include mainly information about the properties of those receivers, about how they work, but it will also include more specific data of the observables of the radiation each different receiver is trying to seek from the threats in the atmosphere surrounding the aircraft. EWSP systems are part of the study in terms of the most significant, and seeks nearly-tymään The main research question answers.

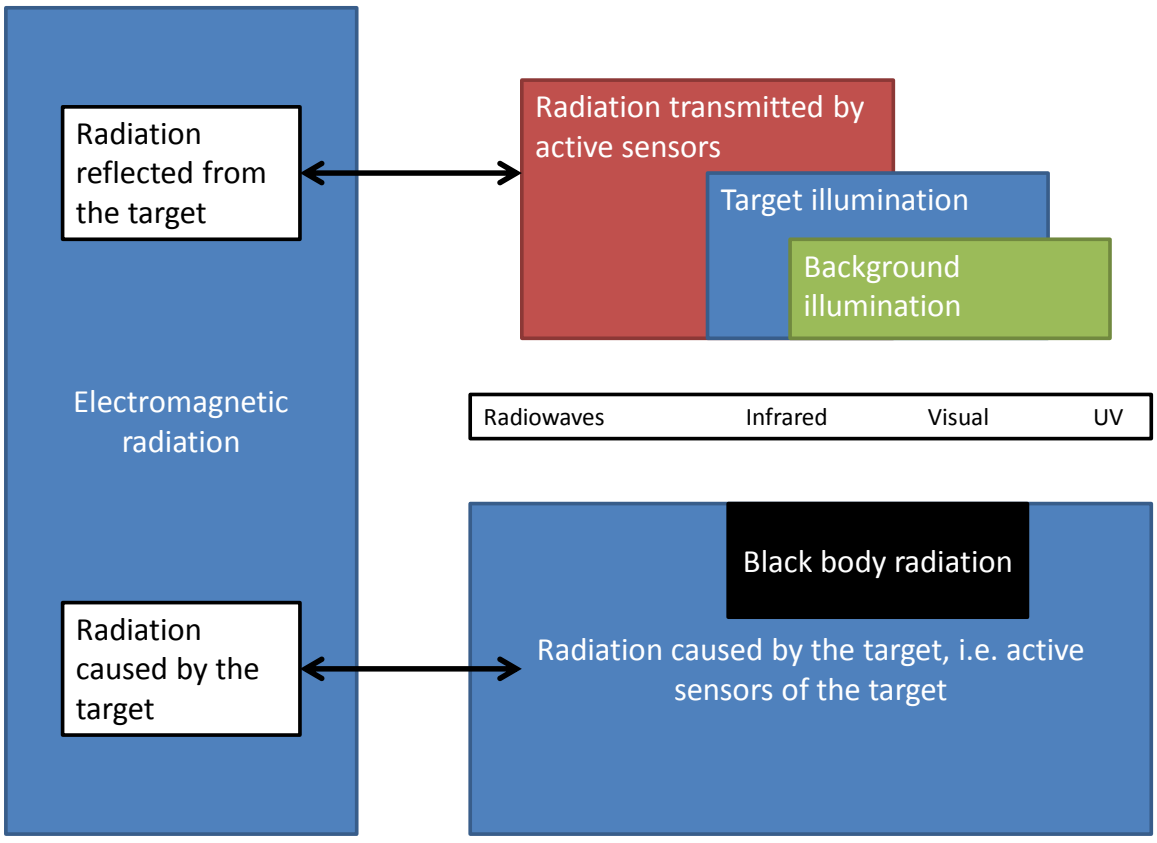


Figure 8: Electromagnetic radiation reflected from the target or caused by the target. Source: Kosola & Solante [16], via Rantakari [17]

3 RECEIVER SYSTEMS OF EWSP

3.1 The purpose of EWSP

Warning system's function is to detect approaching or threats and to alert the protected entity about a near-term danger, which could mean a nation, aircraft, ship, ground vehicle or soldier. A typical scenario where warning systems act involves (1) a platform, or area, to be protected; (2) an immediate danger; and (3) an environment containing a variety of benign objects or events that must be distinguished from the potential threat. Usually a warning system is never off-line, covers a wide range of the electromagnetic spectre and covers a broad range of threat parameters. [18] Heikell has made a well demonstrative figure (Figure 9) from the events and actions in the EWSP countermeasure process. For a reminder, this paper will contribute only in the part where the EWSP detects and tries to identify the signals as a real threat. Other processes are only mentioned.

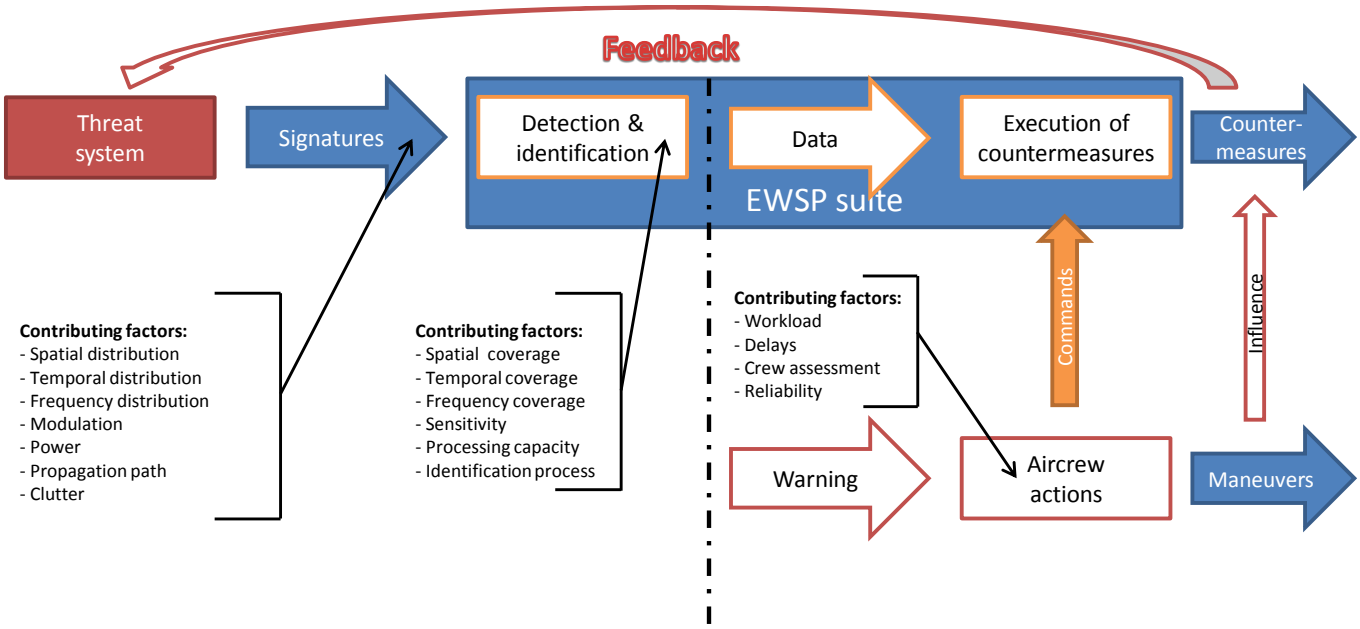


Figure 9: Events and actions in the EWSP countermeasure process, and major factors involved in the process. The influence of CMs and maneuvers on threats is shown as a feedback loop.[11]

Warning the platform involves continuous observation of the environment surrounding the platform, detection and recognition of threats, knowledge of the detailed characters of all the possible threats, and alerting the platform. To avoid false alarms the characterization must be

of high reliability, and it's crucial for engaging the appropriate countermeasures or other actions. After the warning system has done its work and alerted the platform of the forthcoming threat, recognized and located it, the subsequent defensive actions are a matter of other elements of the platforms self-defence, just as pictured above.[18]

Two main missile threats for an airborne platform can be detected through their laser radiation signature or passive signature. Passive signature is the emitted radiation from heating and exhaust products. The missile itself produces heat from friction between its hull and fins and the atmosphere it's travelling through at its usually 2–4 Mach speed.

Next sub-chapters will deal with these main methods each: the missile warning receiver (MWR), laser warning receiver (LWR), and radar warning receiver (RWR).

3.2 Missile warning receivers – Taking Advance of the Infrared and Ultraviolet bands for Detecting Approaching Missiles

At first in these sub-chapters is introduced the passive missile warning receivers (MWR) from all sensors. First subchapter deals with the features of receivers, and their measures of effectiveness. In the second chapter is introduction to the observables of the MWRs. The missile plume is the key for a passive MWR to detect threats, and focus in this chapter is solely on them, such as AN/AAR-44A shown in Picture 1.

Notice, that missile warning systems taking advantage of active radar in detection of threats, like Israeli Rafael's Trophy [19] or French Thales' MWS-20 [21], are limited out of this paper. Advantage of those systems is undeniably their ability to detect threats regardless of the missiles burnout conditions. This regardless of the presumable factor that those active systems could be interfered like an air-surveillance radar. Still, a short description of the active systems is included here. What is in common with land vehicle and airborne active radar missile warning systems is the calculation: they detect the threat approaching the platform, and "perform direction-of-arrival, time-to-impact and missile range, speed and bearing calculations" whether the projectile, missile or RPG, is going hit or cause danger to it. Many systems see much more than on what they take action on, or at least that's what they are presumably designed to do, and not be bluffed with possible threats that are not going hit it. This is actually a major reason why active radar based systems are excluded from this paper. Some methods must be cut out, and this is it.

MWRs differ from the other sensors in its philosophy: it's not capturing radiation which is transmitted on purpose, but only emitted heat, visible, and ultraviolet radiation from the missile's plume, and skin parts that heat from friction. At this point the idea of distracting a passive MWR seems to become an overwhelming task to succeed because of its nature to search of certain kind of emitted radiation but, nevertheless, the process will be unveiled here and solutions shall be tried to be found.

Picture 1: AN/AAR-44A missile warning system. A sample of a MWR that is capable of multicolor IR detection technology for what Jane's calls "a 'positive' missile warning with a 'minimum' false alarm rate". System features include: with (left to right) control display unit, conical detector head and processor. It can detect multiple threats simultaneously with better than 1° angular detection. AN/AAR-44 can automatically visualize and give audial warnings of the threats, and command the countermeasures. The upgraded AN/AAR-44B is described by manufacturer as providing even longer range,and "threat verification against both air-to-air and surface-to-air missiles." Source: Jane's [20]

3.2.1 Features of missile warning systems and measures of effectiveness

Many types of warning equipment and scenarios exist, if looking from a wide angle. These include such devices as fire alarms, nuclear reactor safety alarms, and laser radars. Still, in this paper will be introduced only the ones involved with warning the platform, aircraft, about an attack in process from adversary platform. In the cases treated herein, the emission of visual, infra-red, or laser radiation are characterizing the attack. Warning receivers can be divided into tactical and strategic groups in almost every part of EMS they are working in. If the receiver is mounted on aircraft or any other vehicle and its purpose is to protect that individual vehicle, and maybe the closest ones, it is very clearly a tactical system. The threat is usually a terminal threat such as a surface-to-air missile attacking the protected vehicle itself or other troops and/or vehicles nearby. A satellite-borne IR-receiver, which is designed to detect intercontinental ballistic missiles (ICBMs) is without a doubt considered a strategic system. [18]

Missile warning receivers have traditionally been working in the IR-region and taken advance of the inadvertent emissions from the threat missile. Contemporary warning receivers are working in the wide optical spectrum from the ultraviolet to the far infrared region. MWRs most important region is still the mid- and long-wavelength infrared radiation from heated missile parts and exhaust products. [18] A warning system working only in a single area of EMS couldn’t possibly be very efficient. MWRs work together with systems operating within the millimetre and microwave regions to give a cover as impenetrable as possible. The spectral nomenclature used in this work is in Table 8. Table lists some measures of effectiveness (MOEs), that are best associated with MWRs. There are also defined the typical and desirable values of the MOEs.

Table 8: Spectral nomenclature used in this chapter and later in paper. Via Wilmot .[18]

Band name	*Wavelength (micrometers)*		
Vacuum ultraviolet	0.05		0.20
Short ultraviolet (UV-C)	0.20	-	0.29
Solar blind ultraviolet	0.25	-	0.28
Middle wave ultraviolet (UV-B)	0.29	-	0.32
Long wave ultraviolet (UV-A)	0.32	-	0.40
Visible	0.40	-	0.70
Near infrared (NIR)	0.70	-	2.0
Short wave infrared	2.0	-	3.0
Middle wave infrared (nominal 3-5 urn)	3.0	-	6.0
Plume band	4.0	-	5.0
Blue spike band	4.1	-	4.3
Red spike band	4.3	-	4.6
Long wave (far) infrared (nominal 8-12 ^m)	6.0	-	15.0
Extreme infrared	15.0	-	100
Near millimeter wave	100	-	1000
Millimeter wave	1000		10 000

*

Table 9: Measures of Effectiveness and typical or desirable values. [18]

MOE	*Definition*	*Typical or desirable values*
P_D	Detection probability	0,95–0,99+
FAR	False Alarm Rate	1,0–0,1 /hr
FAR_n	Noise induced FAR	10^{-3}–10^{-4} /hr
FAR_c	Clutter induced FAR	10^{-1} /hr
R_d	Detection range	1–10 km
R_{dec}	Declaration range	1–10 km
FOR	Field of regard	0–360° az ±45° el
DOA	Direction of arrival resolution	±45° az
TTG(TTI)	Time to go (impact)	1–30 s
TTI_{max}	Warning time (maximum TTI)	2–30 s
V_{mc}	Missile closing velocity resolution	± 10 m/s
N_m	Number of missiles handled	< 10
Prioritization	Ability to prioritize among multiple threats	Yes
Latency	Processing time - detection to declaration	0,5 s
Blanking	Blank after detect or CM activation	Yes
NEI	Noise equivalent irradiance (sensitivity)	Band dependent
Altitude	Min. & max. operating alts.	0–10 km
Outputs	Signals to human or CPU	

The efficiency of MWR-systems is achieved by knowing from which wavelengths of EMS is expected the radiation to be emitted from when a missile is launched and during its flight. Missiles do generate very characteristic emission in the optical bands. They are inadvertent, and very vital for the detection of the missile. Water vapour and carbon dioxide molecules account for much of the exhaust emission. The well-known bands from $C0_2$ and H_20 are 4.3 and 2.7 µm, but in addition there are a wealth of transitions in the visible and ultraviolet spectral bands. Some of these originate from the fuel constituents. A few of the more common line

emissions found in missile plumes are listed in . Atmospheric transmission properties, detector and optics technology, and background and clutter levels influence the practical use of any of these optical emissions for warning purposes.

Table 10: Common Plume Spectral Lines [18]

Wavelength (µm)	*Origin*	*Comments*
15	CO_2	
6.3	H_2O	Intense, heavy attenuation
4.9	CO_2	
4.3	CO_2	Intense, moderate transmission
2.7	H_2O	Intense, heavy attenuation
2.7	CO_2	
2.0	CO_2	
1.87	H_2O	
1.38	H_2O	
1.14	H_2O	

The look angle from the target, here airplane, affects the probability of detecting the missile. A missile on proportional navigation is always seen at a constant look angle from the target and a command-line-of-sight (CLOS) missile appears always lined up with the same point on the ground. Regarding to Pollock et al. “The latter are more difficult to detect because they remain fixed with respect to the background clutter features. The variations in signature resulting from changing look angle may deceive warning receiver signal processors that depend on intensity variations to deduce range and velocity.[18]”

3.2.2 Observables – what the MWR is looking out for

IREO Systems Handbook notes that “Missiles generate characteristic emissions in the optical bands that are inadvertent to their propulsion and vital to the detection and warning process. The most prominent of these are associated with the combustion of fuel during boost and sustain phases.“ [18] In addition to combustion related emissions the skin of the missile itself provides detectable radiation. There is a slight temperature difference between the skin of the

missile and its background, and the skin can reflect radiation, usually coming from the sun, and these two characters could prove to be even more robust indicators for the MWS than the emissions from the plume. The share of radiation coming either from the plume or the skin of the missile varies with the view angle throughout the trajectory of the missile. [18] Rantakari presents the four components of the observables for a MWR:

- heating caused by atmospheric friction
- reflected radiation
- hot engine
- exhaust gases (the plume). [17]

An approximate missile exhaust temperature is 2000 K for a kerosene and liquid oxygen, and the radiant intensity in the $C0_2$ plume band for a vehicle of this type is typically 10^6 W/sr, plus or minus an order of magnitude. If the missile uses solid fuels the signatures range between 10^3 W/sr and 10^4 W/sr. Carbon particles may also be contained in the exhaust plume that emit at a temperature approximately equal to the exhaust gas temperature, and act as graybody emitters. [18] It is quite obvious that the radiation intensity of the missile signature depends on the type and size of its motor. To calculate the intensity of radiation in any of the optical bands the *IREO systems handbook* gives a few equations for calculating the intensity *I* in watts per steradian. First, rough and simple, equation for scaling missile signatures is

$$I = kN\ ,$$

where *k* depends on the spectral band. If the intensity is set proportional to the power of thrust the equation would be

$$I = kN^{\alpha}\ ,$$

and the result will be more realistically scaled. In the Figure 11 is shown thrust versus time for several real missiles. The IREO handbook doesn't state any sources to the figure but I have no reason to doubt its value in this research and use. The main duty of it is to demonstrate the fact that missiles thrust is not maintained constant through their flight. A scaling law

$$I = I_{90}\sin(\theta + \Phi)\ ,$$

takes notice of the viewing angle and how it varies the observed signature. [18] Here the I_{90} is the intensity measured from 90° angle to the side of the missile's flight path, the viewing angle. θ is the azimuth angle of the observed angle and ϕ is a small correction, an offset angle. Its value is dependent on the geometry of the missile and its plume. The arguments in the article give the impression that the equation would apply only in cases where the missile is at the same altitude from the observer, that is, the point of view of the aircraft. My impression is that it could be used in situation where the azimuth angle from missile to the observer is zero, meaning it flies directly towards the target in two-dimensional meaning, but its altitude would be smaller or greater, and the altitude-angle would be used instead. In my point of view that's how it is and the IREO handbook only simplifies the equation. What is meaningful is the viewing angle to the flight path of the missile, not whether its to the side or to the top.

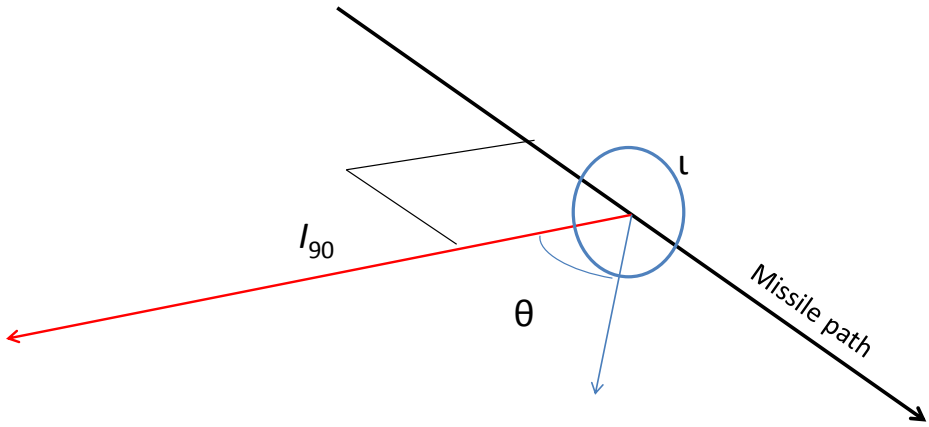


Figure 10: Radiation intensity of the missile plume. I_{90} is the intensity measured from 90° angle to the side of the missile's flight path; .θ is the azimuth angle of the viewer; ι is the yaw angle, which doesn't have any effect to the calculations. [18]

Visible waveband detection is, as mention before one of the methods to detect the threat missile. It may be based in two different sources of light: 1) the emitted light from the rocket plume or 2) from the missile body's scattered ambient light. In the first case is a lot similarities to the infrared band, and the plume intensity is somewhat proportional to power of the thrust. In order to detect the missile in the visible region, as in the second case, there must be sufficient contrast in reflected ambient light between the missile and its background. The reflectances of the target missile depend on the outer surface of the missile skin. The surface may be painted in a way it reflects light as much as a natural background would, so to achieve as small contrast as possible. Usually the missiles are painted or coated with other protective material rather than just leave the skins polished bare metal visible. [18]

The knowledge that in the visible region it is possible to detect the incoming missiles brings a possibility of a new element to the thesis. At this point it is still too early to decide if I'll examine the subject as a one possibility of its own or report of it on the analysis chapter together with other regions which the EWSP utilizes. As early as in the introduction I considered the idea of using dummy rockets to draw the aircraft attention and cause a false alarm. For now I can say for sure that if they are to be used their requirements should include a maximum real-like surface material or paint, just as their real examples, so that the EWSP would consider them as a real threat.

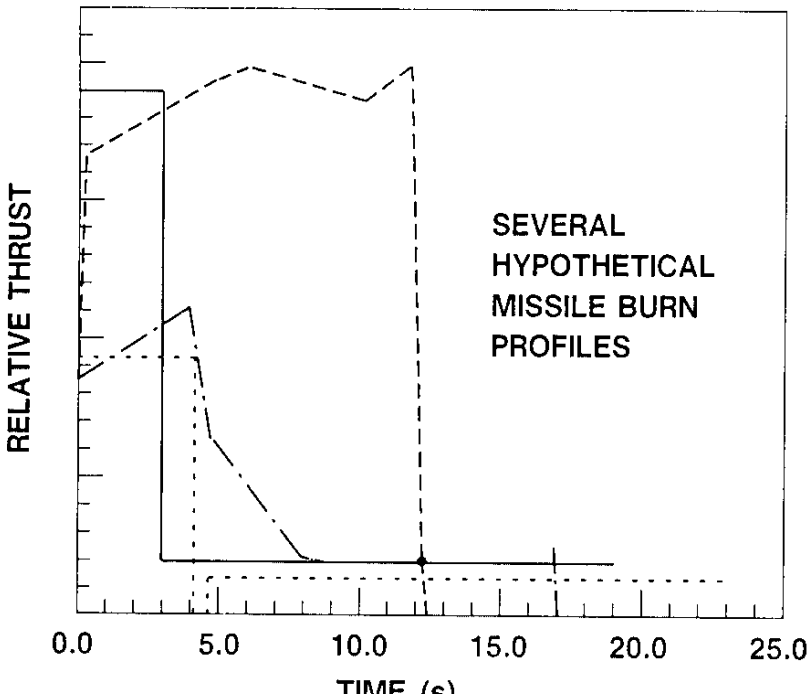


Figure 11: Thrust versus time for several missiles[18]p.21

Steady optical sources, such as battlefield fires, which can be difficult problems for a missile warning receiver, are readily rejected by the transient-oriented circuitry of typical laser warning receivers. [18]

The third region of ESM that is possible to use in the missile detection is the ultraviolet band. IREO handbook shows how a certain jet fuel ultraviolet emission in a region about 220 to 320 nm. (Figure 12)

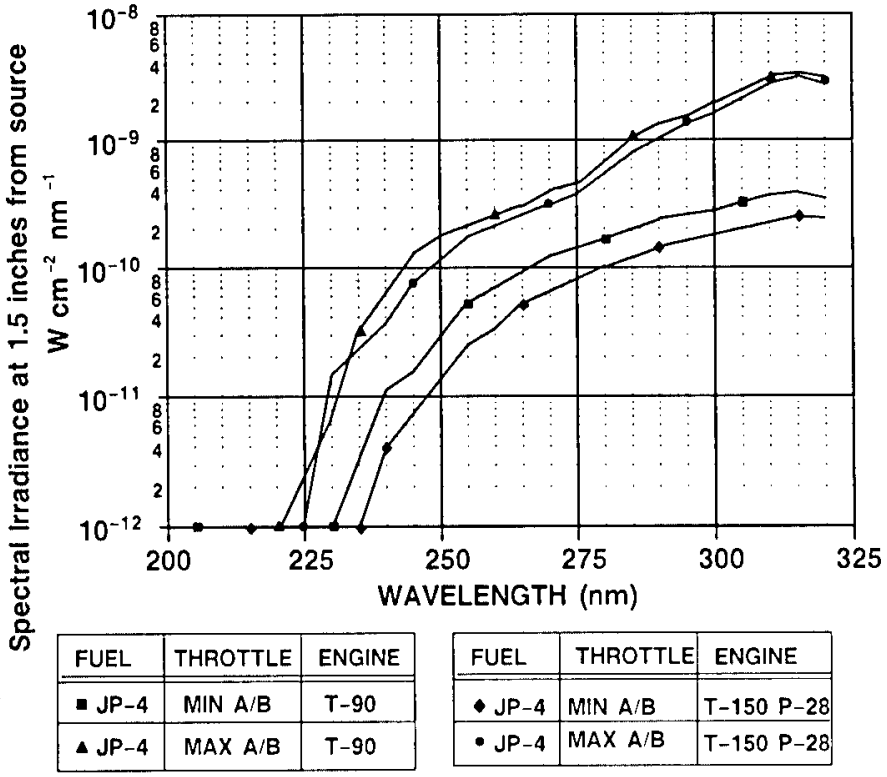


Figure 12. Example of UV spectral data from a F404 jet engine, via Wilmot [18]

3.2.3 Discussion of MWR systems

Passive MWR systems are one of the electronic means of detecting missile launches on the surface, or from another aircraft. An alternative is the mm-region radar intended to detect and calculate the flight path of missiles flying towards the aircraft, but they were excluded from the study.

Missile launch produce a plume that emits from to its surroundings in the IR region from 1.14 μm to 15 mm. Sensors react to the radiation in the visible region, as well, but even if the subject of this extension to the paper would be extremely interesting, it must be dropped out of this study. The radiation in the ultraviolet band must also be taken into account, even though Ireo handbook passed [18] the matter rather quickly in one short paragraph.

The starting point for a missile deception is the determination of the radiation emitted by the missile which is to be “acted as”. The measurements must be as comprehensive as possible in all regions of the ESM specter. Otherwise it might not be credible, and one does not cause any intentional false alarms to the EWSP. A question is, could it be possible to transmit the radia-

tion plausibly enough so that the EWSP would warn the pilot. Research for this paper has not been able to answer that. Answer will not be in this paper, but is a start for a new research.

3.3 Laser warning receivers

Laser warning receiver is not really a piece of equipment that makes the aircraft too much safer above the battlefield. When laser is used on a AA-gun, or tank which is capable in shooting aerial targets, the shells are only seconds away. The function of the LWR as protective device of the aircraft is limited, as Heikell points out. [11] He adds: "A further motivation for the LWR can be found if the EWSP suite is able to correlate data from multiple sources in order to decrease ambiguity of threat identification."

3.3.1 LWR systems and measures of effectiveness

Laser warning receiver (LWR) is applicable for almost any platform: fixed wing arcraft, helicopters, ground vehicles, ships, and satellites. Their function is to alert the platform of impending attack involving fire control, or weapon, lasers; they also may directly activate appropriate countermeasures. Laser receivers are used both for self-protection (i.e., warning) and general monitoring of the adjacent field of battle. Example of Saab EDS system is in the Picture 2. Latter is termed electronic support measures (ESM) in the electronic warfare (EW) community.[18]

In a EWSP application the task of LWR's is to detect the signal, discriminate signals from false signals, characterize the laser, and locate the source of the laser. Table 11, adapted from IREO Handbook by Wilmot, presents common measures of effectiveness. Wilmot also sais the "signal detection is related to system sensitivity and is usually limited by solar-shot noise and Johnson noise in the visible and near-IR regime and by detector/thermal noise in the mid and far infrared. [18]" The sensitivity of the sensor seems to be very critical and difficult to succeed part of the system. They point out the problem with the LWR is in the way the energy of the laser hits the sensor. It could, on the other hand, in different situations come directly from the transmitter, or by after scattering from other nearby objects, so the signal level range from 4 to 10 orders of magnitude, and how it reaches the receiver and how far is the transmitter has a great value. Thus dynamic range in sensitivity is an extremely important feature for a LWR receiver, Wilmot points out, and continues by telling a few good reasons: the signal should not destroy the receiver nor cause any saturation effects that could give incorrect analyze in the signal characterization. [18]

Picture 2. A wide wavelength covering Saab Electronic Defence Systems LWS-300 sensor system: the Threat Display and Control Unit (TDCU) (lower left) with the Electronic Warfare Controller (upper left) and the four sensor units (right). Source: Jane's [22]

Wilmot's text is a couple of years old already, which gives the idea that when he mentions the coherent detection techniques in LWR sensors as a cure for better false alarm rate they must be in more common use contemporarily. If the sensor is not utilizing coherent detection techniques it's very sensitive for giving alarms from virtually any transient light source. For example, sun glint, lightning, gun flashes, explosions and various optical beacons. Usually total immunity to all false sources is desired. What needs more attending to is to get clear what Wilmot means by saying "most LWR specifications include an appropriate electromagnetic interference (EMI) requirement."

To accomplish its task the LWR must be able to do coarse measurements of laser wavelength, intensity, duration, and pulse repetition frequency. These features and the values the signal gives help the LWR to make conclusions between weapon lasers, designators, rangefinders, countermeasure lasers and communication lasers. The LWR converts the data into discrete groups, *bins* it, for threat recognition. Localization of the threat with LWR has some issues and it can be very difficult because of the potential ambiguity caused by the photons incident on the receiver. If the beam comes directly to the receiver the task is quite easy, but when the photons are scattered in the atmosphere, or from other objects nearby, and hit the aircraft from

different or even multiple directions the task is not a simple one, for accurate localizing I would guess possibly even unmanageable in some situations. Wilmot adds that in most situations usually at least quadrant localization is required from the system, but for airborne LWRs a few degrees accuracy would give only an adequate grade and for precise counterattack methods require an accuracy of less than a milliradian. [18]

Table 11: Measures of Effectiveness of laser warning system (LWR) and Common values of.

Measure of Effectiveness	*Common value*
Sensitivity	10^{-6} to 10^{-3} W/cm2
Peak Signal for Correct Analysis	1 to 10^{3} W/cm2
Dynamic Range (Analytic)	10^{4} to 10^{8} irradiance ratio
Dynamic Range (Destruction)	10^{8} to 10^{12} irradiance ratio
False Alarm Rate	1 per hour or per day or per mission
Probability of Detection	0,9 to 0,99
Spectral Resolution	Band to 0.01 µm
Temporal Resolution (Duration)	< 100 ns
Temporal Resolution (PRF)	1 to 10^{-3} s
Temporal Resolution (Interval)	10^{-1} to 10^{-7} s
Direction of Arrival	1° to 45°

Heikell has collected a very good table of questions considering the LWRs and their efficiency. He approaches the difficulties from a slightly different angle, more hands-on type on Table 12.

Table 12: Major challenges in LWR technology and alternative solutions, according to Heikell.

LWR challenge	*Solution*	*Note*
Suppression of false alarms	Pulse rise time.	Not entirely reliable due to rapid sun glithces, especially from helicopter's tail rotor.
	Pulse energy.	Challenging, since the dynamic range of LBR beams and indirect LRF splashes (low energy) and direct LRF hits (high energy), is 50 dB (optical) or more.
	Polarization.	Complex measurement techniques, false alarms from partially polarized non-laser sources.
	Signal coherence.	Military lasers are on ly partially coherent since the focus is on beam width, bandwidth and power density.
	Sensitivity.	Very high sensitivity would allow determination of TOA between direct port scatter and indirect main beam.
LBR signals	Sensitivity.	Tradeoffs required to achieve 10^{-5} W/cm^2 or better; related to false alarm rate, bandwidth, dynamic range, etc.
AOA resolution	Detector array.	Old single detector LWRs achieve only ±45° resolution, new systems reach ±1°. True need is a controversial issue.
Wavelength band	--	Typically 0,5 µm to 1,6 µm, addition of MWIR and LWIR bands increase costs and complexity.
Wavelength resolution	Multiple detectors.	Two partly overlapping detector wavelengths resolce total band in three parts (Si & Ge diodes for 0,5 µm – 1,6 µm band)

3.3.2 LWR observables

The observables of a LWR system are by Wilmot's classification so called basic source parameters, coherence, and radiation patterns. Under the term of basic source parameters are put the features determined by the laser material, the laser cavity or resonator, and the laser pumping mechanism. The choices of configurations for individual applications are selected to accomplish the required task for the laser. These parameters are the wavelength and the purity of it, the polarization, and the beam width. [18]

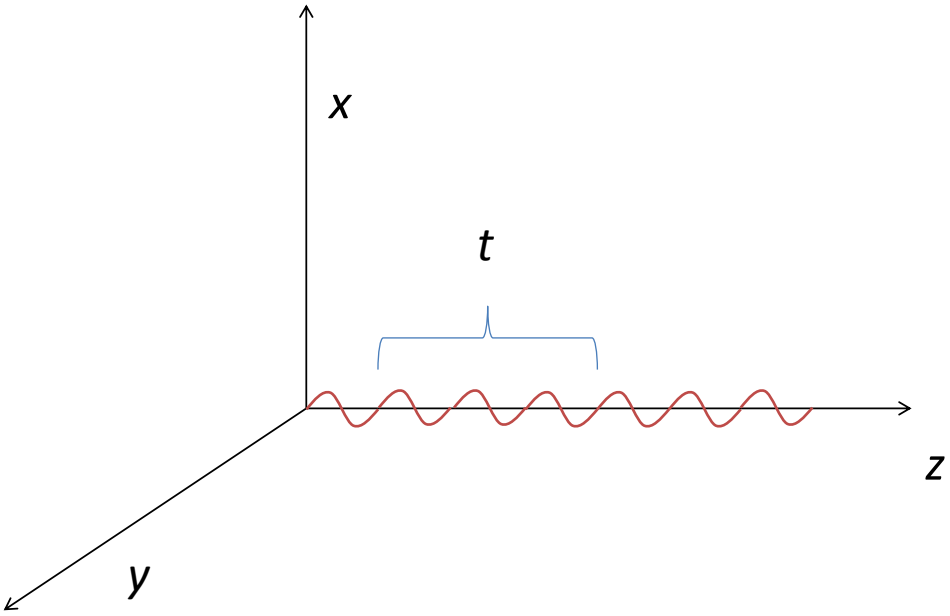
Mainly the factor that determines what is the laser wavelength, is the laser material inside cavity resonator. All individual materials cause individual laser "lines". The material of the cavity resonator has also an effect on the polarization of the laser beam: gas lasers are usually linearly polarized, but many high energy, solid-state, military lasers are unpolarized. Atop that the modal properties of the laser affect the polarization, purity of wavelength, and beamwidth. The more the laser's output power is increased, the single-mode power output is limited by various optical and thermal imperfections and nonlinearities. That is why tactical military lasers are often highly multimode devices. [18]

Some of the relations of the temporal structure important to laser discrimination and recognition processing are next explained briefly. Military lasers currently in use can be temporally characterized as continuous wave (CW), long-pulse, or short-pulse lasers. CW lasers are used in communications or missile guidance, and they usually are gallium arsenide semiconductor (GaAs) lasers or CO2 gas lasers. Modulations from kilohertz to gigahertz are used. In military applications the GaAs-lasers are mainly used in missile proximity fuses or potentially in rangefinders. Long-pulse lasers are used for laser illumination and weapon systems are applications where high energy is important. Ruby and neodymium:glass lasers can be pumped with a burst of energy, and they then lase their normal relaxation time of their laser medium. The duration of the pulse varies between 0,10 – 0,50 ms, compared to 15 – 30 ns of the short-pulse lasers. Short pulse lasers are used when the short duration of the pulse is important atop the high peak power. With Q-switch technology short times as mentioned are possible to achieve, and is the commonly used method in the Nd:YAG rangefinder lasers, and pulse repetition frequency may, according to Wilmot, vary between 1 Hz and tens of kilohertz.[18]

One of the main observables of LWRs' is the coherence of the laser beam. It is process in four dimensions, and they can be envisioned in following way: propagation during time *t*, beam direction *z*, and orthogonal expansions in directions *x* and *y*, as demonstrated in Figure 12. "When such a beam originates at a source that radiates at precisely the same frequency (wavelength) at all times, the wave travels regularly with the instantaneous intensity at each point along the direction of propagation and is totally described in terms of the intensity at the source at that instant and the number of wavelengths, or partial wavelengths, between the source and the observation point [18]." The biggest challenge with fully coherent radiation is with the frequency. If it changes on a random basis at least slightly it affects the regularity of the beam as well. The coherence of the beam, the electromagnetic field of two different observation points being consistent, is therefore never totally perfect but constantly varying over

some range of frequencies. All real sources are somewhat imperfect and their beam has a linewidth typical to its source's physical quality, and features such as laser material. *Coherence time* or *temporal coherence* refers to the duration of the beam being coherent, and *coherence length* to longitudinal distance along which the beam travels during this coherence time, respectively termed *longitudinal coherence*.

Figure 13: Envisionment of propagation of electromagnetic waves in four dimensional process. Legend: t = time, z = direction, x and y = orthogonal expansion dimensions of the beam. Source: via Wilmot & Co. [18]



Laser beam are also characterized as areal sources, or point sources. Conventional optical sources are usually behaving as area targets. Point source laser device is coherent single-mode model. They are usually capable in diffraction limited radiation. Conventional laser mainly have a cone-like radiation pattern. [18]

It is difficult to make quick, hasty and accurate decisions on laser warning receiver data found in the literature. Thought, that the laser beam is fully coherent, and because of that feature, always being distinguished from all other radiation in the atmosphere, is clearly not right. The data presented by Wilmont suggests that quite clearly. Since the laser beam is not completely "clean" also the receiver needs to distinguish not only fully coherent beam as a potential threat. In the contemporary battlefield the use of lasers is in favor of a very large number of

weapon systems due to its accuracy as a distance measurement tool. Laser range finders are in use on the anti-aircraft weapons systems, combat vehicles, anti-tank, artillery observe, and scouting teams, and as well as with any other user who needs accurate distances measured in the changing circumstances and locations. Atop the LRF, no other significant military equipment utilizes laser visibly to airborne surveillance than LBR-systems, as mentioned before.

3.3.3 Discussion on the laser warning system

The literary study of laser warning systems showed me that to deceive them may have one quite fundamental problem: they are not likely to be enough by themselves, especially when trying the misleading against low-flying airplanes or helicopters. LWS's are designed to warn of laser radiation hitting the sensors, which can hit it either directly or reflected in any other subject, as described earlier. I figure at this moment that low flying airplanes and helicopters have even a high probability to alert from laser radiation several times during the task. My conclusion therefore is that, in order to ensure credibility of the ploy, the LWRs are not sufficient enough alone to take advantage when trying to mislead the pilot and the EWSP aboard. Naturally in real combat situations the final results are affected by many factors, such as I have outlined in my introduction chapter.

When the LWS is continuously alerting the pilot of the possibility of a threat it reduces the real threats vicinity and EWSP's possibility to do a correct threat evaluation. Thus the probability increases for a threat on the ground to get lost in the masses and stay undetected; possibly to the point it is too late. This is caused with factor the laser is built closely enough to its real-threat model. The positive increase in the probabilities of the match between the EWSP of the aircraft and laser counter-countermeasures would cause improvement the number of damaged or shot-down aircraft, because

- the first warnings of measurements of the distance to the plane with laser rangefinder, used to calculate a preliminary point for anti-aircraft cannon before a single shot is fired,
- the use of a laser beamrider-type missiles' guidance beam go unnoticed.

More analysis and comparison between receivers and methods is conducted in the chapter 5.

3.4 Radar warning receivers

Radar's (acronym for RAdio Detection And Ranging) function is, in short, to detect a target regardless of visibility and in almost any weather conditions by transmitting radio waves and listening to their echoes. If the waves are concentrated into a narrow beam, the direction of the target can be determined. Range is calculated from the measuring of the transit time taken for the wave to travel to the target and back to the radar. By repeating the sweeping of the radar beam the radar can detect the target. Once found the radar can start tracking the target either manually or automatically, which is a standard method in contemporary radars. The

Picture 3: Spanish Indra made 0.5 to 40 GHz band radar "new generation" warning receiver, that is in operational use in many plane and helicopter types, including Finnish Airforce's EADS CASA C-295. [23]

radar calculates targets relative velocity by computing either (a) periodic samples of its range and direction obtained during the scan or (b) continuous information obtained by focusing the antenna on the target.

“The radar warning receiver is based on receiving radar wave area electromagnetic radiation.” [17] The thing is undoubtedly so, but a little more depth to the matter should be taken in following chapter. It has commonly been said that air-surveillance radar is visible from hundreds of kilometres of distance the moment it starts transmitting. It’s not the purpose of this paper to proof that argument, but airborne radar warning receivers can be presumed to notice a transmitting radar even further than the range of it. Some calculations with this dilemma of the radars is done in the conclusions.

With an airborne RWR the crew of the aircraft notice the activity of the hostile air-defence, and if the radar parameters are well known, could possibly even recognize the source with accuracy of exact air-defence system.

In this chapter will first be introduced the work and measures of effectiveness of RWR systems. Second paragraph sweeps quickly through radar jamming methods, for they are important partner of action with the receivers: EWSP includes jamming of the threat radars or radars of threat missiles trying to hit the aircraft. Last sub-chapter deals with the observables of RWR’s.

3.4.1 Radar warning receiver systems and measures of effectiveness

According to Wiegand the general requirements of EW radar warning receivers are based on three major factors: EM wave signal characteristics, geometric characteristics, and output uses. EM wave signal characteristics are maybe the most important factors, and they include

- “threat-radar signals,
- friendly signals,
- commercial and other signals,
- signals from the asset being protected, and
- jamming signals [15].”

Geometric characteristics are also very important, and might have some influence later in this paper. Continuing the list made by Wiegand there are included characteristics as

- “transmit antenna patterns,
- receiving antenna patterns,
- distances,

- propagation factors such as atmospheric loss,
- background clutter,
- multipath, and
- horizon and line-of-sight issues [15].”

The output uses determine the usage of the data collected by the receiver. Wiegand suggests [15] they should be closely coupled with some parameters of the receiver requirements. This information could become a useful later in the discussion part of the RWR, or they could be more useful for questions dealing with the countermeasures against radar. Still, there has only little found of the inner life of EWSP systems, and them taking advantage of the data collected with RWRs, and therefore they are not going to be dealt any further in this paper. Nevertheless, the requirements of the output uses are, as Wiegand lists them:

- “trigger intrapulse or leading edge functions,
- signal-processing functions, and
- jamming optimization or set-on functions. [15]”

Later Wiegand is describing how the EM wave characteristics, signal and geometric, delineated above can be combined in favor of characterizing the input by definition or description of a much shorter list. In that list are

- “individual intercepted threat signals,
- threat-signal density versus frequency, AOA (angle of arrival), and-so-on,
- self-jamming and self-blanking,
- front-end noise and other interfering signals, and
- external jamming.[15]”

Knowledge of the threat system’s radar or radars can be used when defining the radar warning receiver’s requirements. That knowledge itself is obtained from the transmissions of the radar itself or simply its operating manual. When it is commonly known fact [15] that the intercepted radar signals are one major source for electronic warfare counter and surveillance measures, those parameters should be well hid from the foreign surveillance, and not show off with everything, if not necessarily needed; and, the much this paper is concerned, that’s how it is or should be done.

RWR properties also depend on the purpose of the whole system. Electronic support measure system and electronic counter measure system have consistent requirements of the detection of the signal, but the information they provide is different. In some places ECM system must be able to detect the radar signal in side lobes, for example, if the purpose is to interfere with the radar through the side-lobe so that the radar sees the target in a different direction than it in reality is. This method is known as angle deception. On the other hand electronic support measures may require detecting the sidelobes as well with method and in situations, wherein the angle deception is used. Radar countermeasures are briefly dealt in the next chapter 0. At this point must be noted that if deception is effectively used against radars, why not against the attacker using the same methods.[15]

Quite naturally the first thing defined from the received signal is the type of the radar, that is, is search, track, active missile guidance radar, *et cetera*. Classifying the signals can be done by dividing them into coherent or non-coherent, and by the spectrum they use: fixed frequency, spread spectrum, or agile carrier frequency. Signals can often be classified as chirp or phase coded signals by their compression.[31] One key driving factor for EW receivers design is the classification of the duty cycle of the received signal. Duty cycle, or factor, "is the fraction of time the radar is transmitting [24]", and it was mentioned earlier in the Table 6. Duty cycles are classified as continuous wave, high, medium, or low. Higher the duty cycle, is the harder it is for the receiver to notice the signal. [15] In Table 13 are shown some requirements of the receivers.

Table 13: Selected receiver requirements, via Wiegand. Legend: MDS = Minimum Detectable Signal; AOA = Angle-of-Arrival; DSP = Double sideband. Via Wiegand [15]

Parameter	*Typical Value*	*Fundamentally determined by*	*Other determination*
MDS sensitivity	-50 dBm	1) Distance 2) Cross section of asset	Weakest main-beam signal, or weakest sidelobe-signal to maintain track
Sensitivity adjustment	20 dB	1) Threat geometry 2) Need to take early actions	Need to thing signal environment
Dynamic range	25 dB	1) Distance changes 2) Differences in ERP	Main-beam to sidelobe level
Pulsewidth	0.5 µs	1) Size of asset 2) Resolution needed	Radar function and type
AOA Resolution	10°	1) Geometry 2) Jammer ERP needs	1) Signal separation 2) Other DSP functions 3) Transmitter beamwidth
Output interface	50 b/pulse	Jamming use	1) Signal separation 2) Signal ID 3) Jammer set-on values
Cost	10–40 % of ECM	1) Value of asset 2) Degree operated in harm's way	Complexity needed for sensor function
Size and weight	10–40 % of ECM	Nature of asset	Proper balance with other major subsystems

There are quite a few different sensors and receivers available for ECM and ESM systems and they include

- crystal detector receivers,

- channelized receivers,
- frequency measurement receivers,
- angle-of-arrival sensors, and
- tunable receivers.[15]

Crystal detector receivers rely on the use of crystal as detector material, which has a natural, wide RF bandwidth and fast video output response. A RF signal becomes a video signal after its envelope or phase detection. The RF diode —what the crystal actually detector is— rectifies the incoming RF alternating current and sends it forward in the system as video signal that is single-polarity voltage dependent only on the amplitude of the incoming RF signal, not its frequency or phase. Crystal detector receivers are divided into threshold detect crystal video receivers (CVR) and logarithmic-video amplifier (LVA) receivers. CVR is the most commonly used RWR, and is the simplest one [25], and an ECM system may consist of many of these. In CVR system the crystal feeds a difference amplifier, which is an integrated circuit, or chip[26]. The output of this chip is either a logic "1" or a logic "0", and they are designed to change between these two logic states rapidly when the threshold voltage is crossed. In a LVA receiver the video signal is treated differently. The crystal, which measures the amplitude of the input RF signal, sends the video signal to a logarithmic amplifier. Log amp's desired function is to output a video voltage level that is proportional to the logarithm of the input RF power. An LVA needs a separate A/D converter to convert the signal into digital form, because in a modern ECM or ESM system almost every non-RF functions are done with digital processing. [15]

The digital signal processor of the ECM system needs to know the carrier frequency of the radar signal for separating and tracking them. A channelized receiver (or wide-open (WO) RWR [5]) can provide a solution to this. It is practically a bank of CVRs where each of the receivers deals a separate band of the RF signals coming through a RF filter. And each of the CVRs send their video signal to an OR gate. The OR gate will show a positive indication [27] if there is a signal from at least one of the CVRs. Each CVR feeds also a flip-flop which is interrogated by multiplexer, usually one at time. The multiplexer sends the information of from which channel (CVR) it has given a logic "1", and this channel is at the same time a coarse measure of the detected frequency. The CRSs are not the most expensive part of the system, but if an explicit channel width is desired, it could result in major cost increase. Usually the range is 5–50 MHz, and requirements to narrow that include

- the pulsewidth of a typical radar,
- MDS sensitivity,
- frequency selectivity,
- maximum size of the system, and
- amount of assets for the development and purchase. [15]

Instantaneous frequency measurement (IFM) receiver provides an almost instantaneously measured carrier frequency of the incoming RF signal. Its response time is so short that it's a fraction of most practical radar pulsewidths. Crystal detectors are included, once again, but the IFM includes also couplers, a fixed attenuator, and a delay line. RF input signal power is divided in two paths, one of which contains the delay line and the other a fixed attenuator. The attenuation in both lines is nominally the same. They are then combined again with a hybrid coupler which feeds the two crystals. The video signal from both the crystals is changing depending on the frequency. At some frequencies the two signals combining in the coupler are 180° out of phase, and all the power goes to the crystal X. At other frequencies the power goes to crystal Y, "and the pattern repeats across the band."[15] Calculating the frequency is then done by mathematics. [15]

In the analog delay line type described above the amplitude of the input signal must not change with frequency. Twice as many crystals and hybrid couplers are needed to provide automatic dynamic range normalization. The crystals are summed in pairs, and these two pairs then feed an operational amplifier each. Op amp's task is to sum the opposite polarity signals. This arrangement is called an RF phase correlator. The output of the op amps can be shown on a conventional polar display, where X and Y video voltages are shown as coordinates. A more contemporary method is to send the signal next to an A/D converter, and from there it to its utilization. The phase correlator can measure the AOA of the RF signal, if it is made to calculate the phase difference between two antenna elements. [15] At some points the Wiegands book seems a little oldish for contemporary use, but the idea of the receivers work comes clear.

Angle of arrival calculation is important to the ECM and ESM systems, as well. This can simply be made by calculating the amplitude difference between two antenna elements, or like described in the last chapter above. In amplitude comparison the antennas are at slightly different angle, but their main beams are still overlapping. Yet again, the crystals in line with each antenna convert the signal into video signal, of which polarity is then summed in an op

amp. After that the signal is converted into digital form, and send to its utilizer and/or display. [15]

All the RWR methods described above have a useful instantaneous bandwidth of multi-GHz. A sweeping, or tunable, receiver has, on the contrary, a narrow IBW. It is needed when the received signals overlap, and thus corrupt the measurements with receivers described earlier. Tunable receiver can be used to supplement the data from CVR, LVA, channelized, and IFM systems. Wiegand shows to types of tunable receivers: a YIG-tuned (Yttrium Iron Garnet) receiver, and a superheterodyne receiver. The YIG-tuned receiver is made by simply adding a YIG-tuned filter in front of a broadband CVR or LVA receiver, or both. The YIG-tuned filter passes through a certain frequency when a certain amount of currency is fed to magnet in it. The hysteresis phenomenon, the frequency passed through is higher when tuning down than when tuning up at the same currency, is a well-known problem with a YIG-filter, but it's avoidable. [15]

The superheterodyne receiver (superhet) is one of the oldest receiver designs existing. In superhet receiver the RF signal is beat to the intermediate frequency (IF), and then amplified in the IF amplifier. IF amplifier, also known as IF strip, supplies two outputs: discrimination voltage and the video voltage. The video output shows the strength, and the discrimination output shows the relative frequency within the receiver's IBW. The mixer that beats the incoming RF signal is steered from the voltage controlled oscillator (VCO), which again is steered digitally through an A/D convert. Superhet receiver linearity is poorer than with the YIG-tuned receivers, caused by the linearity problems with the VCOs. On other hand, their sensitivity is told to be better than with crystal receivers'.[15]

Radar warning receivers brief overview on this study doesn't go any further. It was a necessity, however, because it is precisely those that main research problem is directed, and the LWR and the MWR. Brief overview of the RWR has brought a lot of information also for future chapters dealing more with RWR observables.

But the radar signal doesn't stay in the receiver but continues further in the system for identification and tracking, for example. These matters, and other involved in the digital processing, will be covered next in this sub-chapter.

When the incoming RF signal has been detected and transformed into video signal, and later into digital signal, begins many very interesting procedures in the digital signal processor of

the RW system. CPU and DSP perform digital processing functions that are shown in Figure 14. It includes the sensor block, for clarity, which is dealt earlier in this chapter. The primary functions of the digital processing are

- “signal processing,
- signal identification,
- signal track and prediction,
- waveform generation, and
- central processing.”[15]

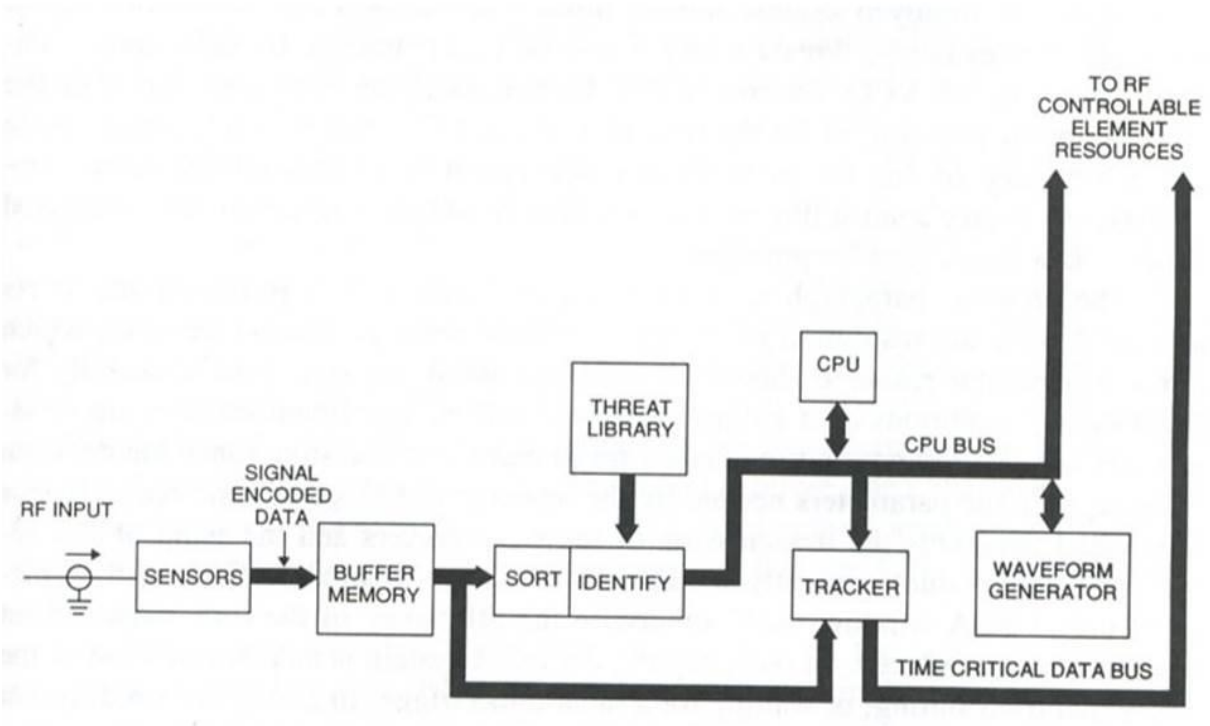


Figure 14: An example figure of digital prcessing functions of a radar electronic counter measure system, via Wiegand.

The central processing unit (CPU) has a variety of software-generated functions that, in time-scale of their actions, include

- technique determination,
- priority conflict resolution,

- resource allocation,
- parameter setup,
- data and parameter maintenance,
- gain and power control,
- slow servo functions, and
- built-in tests.

All of these listed tasks are not shown very interesting for being more than introduced in this paper. The technique determination is simply picking the best-rated technique against the threat that is identified. It becomes difficult if several threats need to be dealt with a preset mode. It actually becomes a problem of the priority conflict resolution and/or resource allocating functions. The system has only certain amount of resources to be used at a time, and priority conflict occurs if there are more threats to handle than resources available. The system is most efficient if it either transmits, or is fully prepared to start transmitting the moment the triggering radar signal is detected. [15].The text gives the idea of the CPU being crucial element of the system as a whole, which though is not a great surprise in a modern world filled with electronic devices.

The signal sorting and identification are dealt more later in the chapter 3.4.3 RWRs' observables. It is a significant factor of determining the signal authenticity, so it deserves its own chapter.

Pulse repetition frequency (PRF) tracker has a duty as one of the means to sort the input interleaved pulse train. Sorting is done for separating or de-interleaving the input signals. PRF trackers predict the moment for transmitting when such jamming is used that needs prediction and exact timing before the triggering signal is received. PRF trackers are very important mechanics in an EWSP system, so there are strict requirements for quality given to them, including

- "TOA gate jitter,
- acquisition time,
- vulnerability to missing pulses,
- vulnerability to interfering signals,
- harmonic acquisition inhibit,
- stagger acquisition,
- vulnerability to multipath induced leading edge modulation, and

- vulnerability and response to agility.” [15]

Wiegand notes the two first criteria being most often mentioned when talking about tracker performance. Usually the tracking can begin with three to four incoming pulses. TOA gate jitter is the other important criteria,[15] and knowledge of these brings a new idea of noticing if the possible deceptive bait is taken: if the opposite side starts timed jamming against used frequencies.

Digital signal processing of EWSP systems, and any systems, is in constant development process. Producing materials are getting better in all aspects, and handling methods of them improve. DPS systems’ performance will continue to advance in the future, but predicting the evolution is not in this papers questions.

3.4.2 Active electronic countermeasures against radar

Differing from the missile warning receivers and laser warning receivers, the radar warning receivers are —at least they could be— used for active electronic counter measures. And it is much more usual than with the first two ones. Radar is, the way the subject seems to researcher, an electronically vulnerable transmitting and receiving equipment, and many different countermeasures are known to be used to blind or distract them. Because of the nature of RWR being part of active ECM, a short subchapter of those countermeasures could be useful and justified, before going any further in the observables of the receivers, and in the analysis of the distracting possibilities of them and whole systems.

A very compact way to determine the active ECM is how Wiegand puts it in his book: “”an active ECM technique” refers to a method used to negate the effectiveness of threat radar systems by transmitting EM radiofrequency signals.[15]” Doing that is properly is not as simple as it sounds; non-active ECM includes evasive actions and moves, dispensing flares to distract electro-optical missiles, or dispensing chaff to blur the RF signals of radar. Other than self-protective active ECM options include methods used for stand-off jamming, and escort jamming, and multiple spatially diverse on-board jammers. Stand-off jamming, namely, “standing out of harm’s way”, is done with large, powerful transmitters from a distance where it is out of the range of close and medium range air defense, or air-to-air weapons. Usually these aircrafts are built solely for this and other EW purposes, and work as protecting the engaging aircraft from a distance. Escort jamming is similar in the way that they are planes equipped mainly to the countermeasures, and those planes are usually carrying very capable and rela-

tively expensive EW equipment with them. Differing from the stand-off jamming craft the escort jamming planes come usually substantially closer to where all the action is, and are thus substantially more vulnerable to the air defense and air superiority fighters. In both cases the craft engaging targets in the battlefield may, or may not have self-protective ECM, or they may not use them. Spatially diverse jammers are on-board those airplanes acting in the battlefield and engaging their targets and thus are very likely to be targeted themselves by the air defense or fighter planes. The cooperative ECM waveforms used in this cost-effective method may be free-running, synchronized with accurate clocks, or with synchronizing communications. [15]

These active ECM systems usually have a set of jamming-deception methods either fixed or set on a mission basis. Wiegand book is more than twenty years old now, so what he mentions about the "modern active ECM systems -- have a repertoire of techniques from which sopisticated double sideband(DSB) subsystems make selections and set parameters in real time." Controlling the ECM electromagnetic waves in time, carrier frequency, carrier phase, amplitude, polarization, and direction suitably is a compulsory. DSB subsystems are not further unwrapped, and for further information of DSB one should be referred to Wiegand's text. [15]

Self-protective active ECM is practically the same method as described above about the other methods, but in smaller scale, and with a smaller task to fulfill. Negating search radar functions, making tracking radars more difficult to accomplish their acquisition modes, negating radar tracking and guidance modes of radar guided weapons, and jamming missile and munition functions. Summary of possible and maybe the most potential active ECM techniques against different radars are shown in Table 14.

As the nature of this sub-chapter was simply to unveil the purpose of the output of the RWRs, not to start a further study of the subject, there will be no deeper knowledge presented. For further reference on the subject one should acquire the Wiegand's [15], Stimson's [24], or De Martinos's [5] book.

Table 14: Some basic electronic counter measures used against different types of radars, via Wiegand. [15]

*For countering a *** radar…*	*…this is a useable technique:*
1) Search	False targets or noise either from spatially diverse ECM sets or into sidelobes
2) Track acquisition	Blinking on and off or switching among jamming techniques
3) Conical scan angle tracking	Transmitting high power except near center of radar antenna main beam
4) Range tracking	Transmitting noise or pulses around (just before, on, and just after) the true target range position
5) Doppler tracking	Phase-frequency modulation to cause a false frequency offset
6) Monopulse angle tracking	Range jamming (#4 above); once the range track has moved to a false range, use data-rate reduction to starve the radar angle track servo so that it drifts off the true angle.

3.4.3 RWRs' observables

Radar warning receiver is made for detecting radar signals. Detection is only the first part of the target acquisition process [28] proceeding recognition. If in detection, as talking of radar signals, the target's presence is noted, in recognition the target has been determined to have potential military interest. Next step is identification of the signal as a military radar signal of search, track, and *et cetera* radar. The target's or threat's location is then tried to be found out. That matter was dealt in an earlier chapter, though. Radar signal identification is hard to be kept separate from recognition, or that would at least be little artificial. That's why only identification will be spoken of later.

During this chapter the will be presented a brief list of the matters the radar warning system, part of ECM or ESM, is truly interested in and from which it identifies an incoming signal to be a real threat among all the RF signals transmitted, and reaching the receivers.

Sorting the signals aims for separating incoming signals from each other, and is done in a processing unit of the radar warning system. Radar signals are transmissions in pulsed or CW mode. Examining the relation between pulses, called pulse-train sorting, is used for low- to medium-duty cycle signals. [See also Table 6 and chapter 3.4.1] Single-pulse measurement is

possible, as well, and both are considered effective. Segregation of pulses into bins is done with parameters

- "RF carrier frequency,
- AOA,
- pulsewidth, and
- intrapulse modulation." [15]

The list above is at the same time the list of the most important signal parameters to get as close to the original radar's parameters as technically is possible, when considering the deceptive transmitter's parameters.

Multidimensional processing is considered as an effective method, as well, and it aims in easing the signal separation's burden. Its advantages are illustrated in Figure 15 below. From top to bottom, the paragraphs represent five pulse-trains A, B, C, D, and E, with unique amplitude, pulsewidth, and PRI; the PRF spectrum; and the RF carrier frequency.

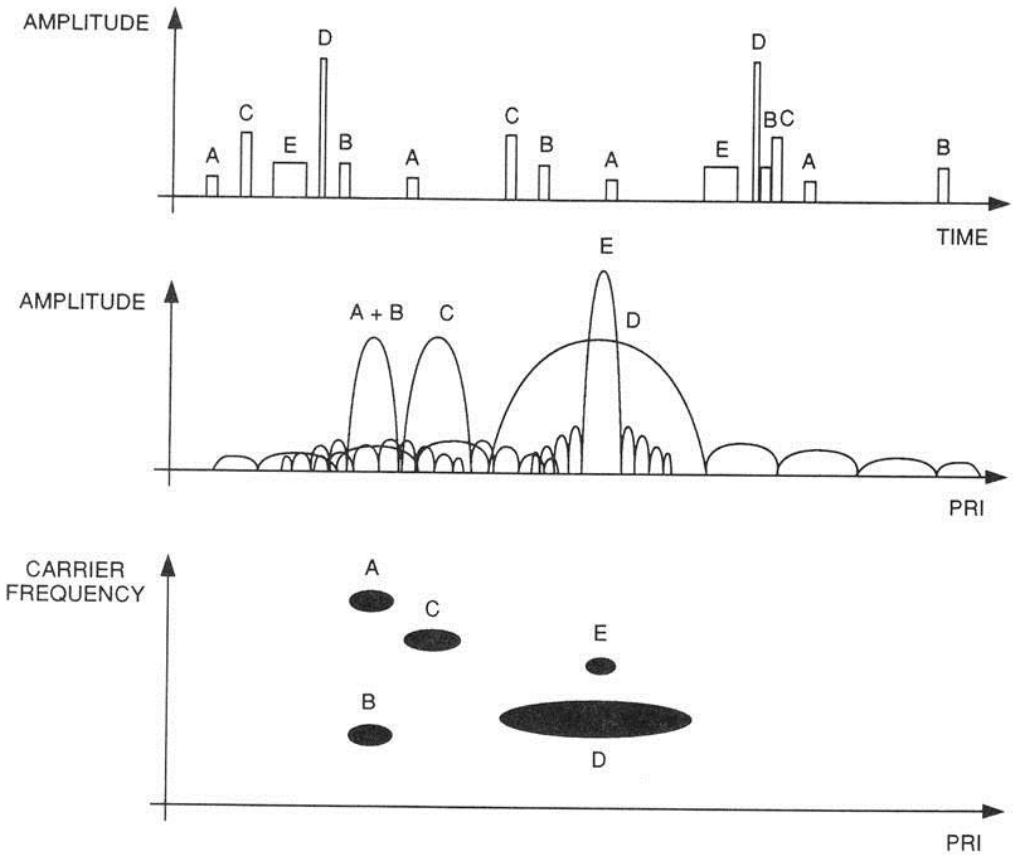


Figure 15: Two-dimensional processing, via Wiegand [15].

It is possible to examine three or more input parameter dimensional spaces with the DSP algorithms, but their visualization becomes difficult. Two dimensional visualization is still easy to understand, such as the graphs of the Figure 15: pulse-trains A & B seem to have the same pulsewidth, but in the bottom graph they are separated because of their different RF carrier frequency.

3.4.4 Discussion of radar warning receivers

RWR system's demand for processor performance appears to be on the most demanding on from the group of different warning systems. In order to distinguish the correct radar transmission from each other, as well as intentionally or unintentionally transmitted ones, and the reflected ones, it must be able to make a continuous, very fast, and accurate work, such as in subsection 4.4.3 is illustrated.

The most up-to-date source of this study says WO RWR system is currently the most commonly used of the RWR systems. De Martino continues that contemporary systems include in growing numbers the IFM system, as well. [5] According to that, there is a reason to believe a RWR of a modern military aircraft has such a combination of equipment *per se*. Worst case scenario -thinking cannot go as an empty exercise here.

It is certainly possible to build a credible deceptive "pseudo-radar" device, if it follows the same idea as with laser and missile deception: measurements must have been done in laboratory environment to make the decoy's radiation transmission identical with its original model. The challenge is, tactically speaking, that the radiation must come from a credible direction. A short example about the effect of the AOA devices impact to distraction: A radar is transmitting, and an aircraft detects the RF signal. Quite clear presumptions can be made about the detection when the aircraft begins trying to jam the radar. If the radar is needed to change to new area, it can be done during the normal alternation and pacing of transmitting. When the radar stops transmitting, the pseudo-radar is turned on when timing is plausible, and the radar can retreat. The situation should look normal from the aircraft's point-of-view. In this case, the risk of anti-radar missile (ARM) hitting its target is radically reduced. Pseudo-radar, however still in the danger zone, is significantly less expensive than the radar. And there are certain known methods to reduce the risk of ARM hitting the radar, or pseudo-radar.

The AOA resolution must be taken into consideration when planning such plots. Wiegand suggests it's typical value is 10°[see Table 13]. Wiegand's book is already ageing in the scale

of EW, and therefore in calculations made in the Table 15 is few different resolutions used. If then the systems communicate between each other, and capable of triangulating the position of radar [29], range maximum between radar and pseudo-radar could become much smaller.

Table 15. Calculations of the impact of different AOA accuracies on the distance between the radar and decoy. Legend: AOA = Angle-Of-Arrival; A/C = aircraft.

AOA resolution (DEG) α	*Distance of A/C (km)* d	*Radar to pseudo-radar range (km)* $R = \frac{\alpha}{360} * 6d$
10	10	1,67
8		1,33
6		1,00
10	20	3,33
8		2,67
6		2,00
10	50	8,33
8		6,67
6		5,00
10	100	16,67
8		13,33
6		10,00

3.5 Discussion of warning systems

Short discussion of each warning receiver is in the end of their sub-chapters, respectively. This closing discussion of the warning systems as a whole is meant to draw short conclusions of observations made in the Warning Systems chapter.

EWSP systems cover the electromagnetic spectre from ultraviolet region (abt. 200 µm) all the way to UHF frequencies (500 MHz [23][30]). Different regions of EMS are covered followingly:

- ultraviolet: MWR
- visual light: MWR, LWR
- infra-red: MWR, LWR
- radio waves (other): not in interest
- radio waves (UHF): RWR
- micro waves: RWR

The answer to the question about different observables of each warning receiver cannot be answered in one simple sentence. Therefore a collection the observables are combined into Table 16 below.

Table 16. Combination of the observables of each warning system.

Receiver…	*…and a collection of its observables.*
Missile warning receivers	* heating caused by atmospheric friction * reflected radiation * hot engine * exhaust gases (the plume).
Laser Warning receivers	* wavelength (and purity of it) * polarization * beam width * temporal characters (CW, short-pulse, long pulse * coherence (temporal & longitudinal) * areal vs. point source
Radar Warning receivers	* carrier frequency * pulse repetition frequency * pulse width * scan type/ Digital beam-forming * bandwidth (BW) * polarization * coherence

4 ANALYSIS OF DECEPTION

In the past chapters are covered the different threat systems, terminal and non-terminal, and EWSP systems aboard the aircraft. EWSP systems design aims in doing the best to prevent the aircraft to end its flight too early. The main task of this paper was to find the best possibilities to succeed in deceiving the airborne EWSP systems. A pressing question "What type of apparatus could do the decoy's job and what kind of requirements for them should be considered?" This chapter will deal with these questions. By answering to the pressing question on each warning receiver the answer to the main research question comes more and more clear.

EWSP is an integrated entity [29] or, at least, should consider as one. Its separate receivers collect information of radiation surrounding the platform that could be harmful against it, or other friendly platforms. Jotta sen harhauttaminen olisi mahdollisimman suuri onnistuminen, pitää eri vaihtoehtoja pohtia mm. panos-tuotos ajattelun avulla.

The missile deception has many challenges. The live missile firing is always a logistical challenge since the number of missiles should be expected to be limited. This is probably reality to all of the armed forces except, perhaps, the biggest military powers that have invested in major financial contributions to their armed forces' procurements. A single modern anti-aircraft missile price today is easily 100'000 €, or more. The smallest shoulder-fired missiles could be cheaper. It could be a financial relief for smaller armies to think that the substitute for a real missile would cost, maybe, a tenth of the original. The plume of this *pseudo-missile* must be designed and tested to be close enough to its model. The MWR system identifies certain wavelengths of simultaneous thermal, visual, and ultraviolet radiation which emits from the plume to surrounding environment.

Other specific requirement of the rocket development work is to consider what happens to it after the rocket engine has burned out. Opening a parachute immediately after the burnout could blow the deception. The pseudo-missile must also have enough intelligence aboard that it is able to be guided towards the target for a sufficient amount in time. Temporal and spatial considerations of the missile's flight must also be done. How long should it fly? How far from the launch pad it is then? These assessments must be made according to the missile's model. The rocket motor burn time could be from two to five seconds, and the total flight time of it from five to ten seconds, respectively.

Expanding the flight time will definitely increase the probability for the MWR to detect this possible threat, warn the pilot, and execute ECM. If the plume is not visible enough for the MWR to notice it, for any reason, the friction heating the skin of pseudo-missile could cause the false alarm instead. Heated skin was another source of thermal radiation for the MWR to react, and visual approach should be thought of, as well. The arguments are proven earlier in the MWR chapter 3.2.2.

A major question arises from this kind of deceptive action: what are the vested interests of this action? The plane could spend its flares or chaff-dispenser [32] for a false alarm, but the pseudo-missile will never make a kill. Though, the real missile systems hit-probability on one-on-one scenario gets higher [13].

The challenges with laser warning receivers are different than of those with MWRs. Earlier in the chapter 3.3.3 was stated the way how a laser beam can hit the receiver directly, and by reflecting from objects in the beam's way. The research has given a varying picture about LWRs in action. They seem to be so sensitive that they alert the system almost all the time the craft is above battlefield and there is no more than one user of laser equipment on the ground. On the other hand their MOE states the FAR of LWR should be less than one in hour. This must be questioned! There could be a simple answer to the confusing situation: the age of the Wilmot's text. IREO handbook vol. 7 was introduced back in 1993 [18], and prices of electronics in general have come down since then. That has made greater number of laser devices in battlefield affordable in greater numbers. This doesn't base on any more profound research than simple reasoning.

Like noted above, the MOE of LWRs are loose enough to make any LSR an possible dummy. Pseudo-laser is not a good name here, because the apparatus would still do its original task, and work as decoy only when decided. Controlling the use of LRFs is another topic. If they are scattered around the battlefield, only general instructions of their use could be given. Controlled large-scale operation against air-threat is presumably going to end unsuccessfully. No guarantee can be given for troops 1) receiving all the instructions and understanding them fully, and 2) remembering or obeying them after days or weeks of combat.

General instruction should be simple: whether to use LRFs against aircraft, or not. Some extra notes could be added, like what kind of situations are preferred, how is own concealments preserved, *et cetera*. But smaller scale operations aiding the use of AAA or other air-defense is plausible to succeed, if it's in hands of smaller group whose aim is simply to give time to

the air-defense teams to prepare their launch. This is achieved by pointing the aircraft a few moments before the group is using their integrated laser device, and continuing doing so for a while longer.

Considering the vulnerability of the sensitivity of LWRs, their use could be more cautious than the use of MWR's. If MWR gives an alarm it should cause action, but when LWR notices the presence of laser radiation it might mean nothing. It could be it has happened many times before on that mission, at least if the ground troops point all possible laser apparatus towards the aircraft flying by, or further off. Consequence of imbuing the LWR with constant false alarms could lead to positive results when a real AAA platoon's or LBR team firing preparations are not noticed. LWRs' real ability to classify beams from each other's wasn't clarified during the research, but that was expectable due to covering of confidential and vulnerable information.

EWSP is not only a passive system. EWSP systems take actions against emerging threats, even only possible such. This means countermeasures against missiles. Flares and chaff are an example of those. It seemed that RWR's priority was to gather information solely for the means of ECM against the threat radar. Using decoys or so called pseudo-radars and some calculations regarding that was briefly presented in the discussion paragraph of the RWR chapter. Imbuing a contemporary RWR is maybe not possible because of contemporary CPU's calculation and multitasking speed. RWR is constantly receiving information, and even Wiegand showed in a figure (Figure 15) back in 1991 how RWR is dealing with five different radars. It could be that number was underrated for simplifying already then, and real multi-radar tracking volume is presumably much higher in contemporary radar ECM systems. ECM system does the actual tracking, and the receivers are, namely, for receiving the signals.

The principals of making pseudo-radar differ in no way of the making of a pseudo-missile: the electronic signature need to be brought as close to the original radar being pretended. This is measured in laboratory environment. The resources used to purchase the EWSP might become actually the most crucial requirement of the RWRs and ECM systems. It is possible that the signal is not possible to make close enough to the radar to keep the disguise against big scale electronic warfare support measurement's. Smaller EWSP systems on the other hand could be bought.

When considering the possible assemblies, uses, tactics, and plausible effects, the best single method against airborne EWSP system is the deception of the RWRs and the ECMs in connection with them.

5 CONCLUSION

5.1 Evaluation of the results

This paper makes good progress in the search of the answer to main and pressing questions. Answers were found to all of the questions but one. During the process many some examples of electronic deception was found [33], but no sign was made of any device for this kind of deceptive action, prototype or in production. Not actually any research that would come close to this paper's subject. This was quite shocking news at first. It brings some other questions in mind: Could it be possible that the subject really isn't examined earlier at all? Or, has it been done and later made decision not to proceed with the subject? Whatever the reason has been, this paper is one solely concentrating on electronic deception of EWSP.

The supplementary tasks are fulfilled with the chapters dealing them, respectively. Threat systems signals and their transmitters are presented in chapter 2. The focus was not in this matter more than was vital in explaining the basis of the whole paper. The second two questions were more important from the main task's point-of-view. They are as much opened as it was practically possible in a brief research as this one. Their answers are split into three paragraphs of the chapter 3, each warning receiver in its own.

5.2 Evaluation of the scientific contribution

Facing the fact that no other research has been made from this narrow perspective, it must be said that the path-opening value for this paper could rise. Still it is too early to determine this papers ground-braking value. Others can do that.

5.3 Suggestions of topics for future researches

One suggestion rises from the idea mentioned in the MWR section: deceiving the MWR with an artificial electronically produced missile launch.

REFERENCES

[1]	*FM 3-05.30, Psychological operations*. Washington, DC.: Department of the Army. 2005.
[2]	*Air Force Doctrine Document 2-5.1, Electronic Warfare. DRAFT.* Air Force Doctrine Centre. 1999.
[3]	Margolis, Eric & Laurence, Stephen: Concepts. Stanford Encyclopedia of Philosophy, 2011. Published: 17.5.2011. [Referred: 13.4.2014] Found: http://plato.stanford.edu/entries/concepts/
[4]	Alm, Jarno. *Pulsed Doppler Radars in Electronic Warfare*. In: Jormakka, Jorma and Rissanen, Antti (Ed:s.). State-of-the-Art in Sensors. Finnish Defence College, Department of Military Technology, Series 1 N:o 24. Helsinki, 2006. p. 112–121. ISBN 951-25-1650-0
[5]	De Martino, Andrea: *Introduction to Modern EW Systems*. London: Artech House, 2012. xiv, 417 p. ISBN-13: 978-1-60807-207-1.
[6]	Frater, M.R. & Ryan, M: *Electronic Warfare for the Digitized Battlefield*. London: Artech House, 2001. 262 p.
[7]	Hirsijärvi, Sirkka; Remes, Pirkko; Sajavaara, Paula: Tutki ja Kirjoita. 10. painos. Jyväskylä: Kirjayhtymä, 2004. 436 s. ISBN: 951-26-5113-3
[8]	Varto, Juha: *Laadullisen tutkimuksen metodologia*. pdf-julkaisu. Omakustanne: 2005. 204 s. [Referred: 13.4.2014] Found: http://arted.uiah.fi/synnyt/kirjat/varto_laadullisen_tutkimuksen_metodologia.pdf
[9]	Tuomi, Jouni & Sarajärvi, Anneli: *Laadullinen tutkimus ja sisällönanalyysi*. 1.–2. painos. Jyväskylä: Tammi, 2003. ISBN: 951-26-4856-3
[10]	Anttila, Pirkko. *Tutkiva toiminta ja ilmaisu, teos, tekeminen*. 2nd ed. Helsinki: Akatiimi, 2006. 674 p. ISBN: 952-5378-11-X

[11]	Heikell, Johnny. *Electronic Warfare Self-protection of Battlefield Helicopters: A Holistic View*. Espoo: Helsinki university of Technology, 2005. 217 p. ISBN: 951-22-7545-7
[12]	Use of helicopters in land operations, Volume 1. ATP-49(c). NATO, 2000
[13]	Ball, Robert E. *The fundamentals of aircraft combat survivability analysis and design*. 2nd ed. New York, NY: American Institute of Aeronautics and Astronautics. 2003. xi, 398 p. ISBN 0930403029.
[14]	*Wavelength chart*. Shanghai Laser & Optics Century Co., Ltd: 2004. [Referred: 13.04.2014] Found: http://www.lasercentury.com/category.asp?id=23
[15]	Wiegand, Richard J. *Radar electronic countermeasures system design*. Norwood, MA: Artech house, 1991. p. 277. ISBN 0-89006-381-8
[16]	Kosola, Jyri & Solante, Tero. *Digitaalinen taistelukenttä - informaatioajan sotakoneen tekniikka.* Maanpuolustuskorkeakoulu, Tekniikan laitos, Julkaisusarja 1 N:o 7. Helsinki, 2000. 402 p. ISBN 951-25-1143-6.
[17]	Rantakari, Riku. *Possibilities of Improving – Situational Awareness of the Tank Crew*. In: Jormakka, Jorma and Rissanen, Antti (Ed:s.). State-of-the-Art in Sensors. Finnish Defence College, Department of Military Technology, Series 1 N:o 24. Helsinki, 2006. p. 63–76. ISBN 951-25-1650-0
[18]	Wilmot D.W., Owens W. R.. Shelton R. J. *Warning systems*. In: Countermeasure Systems. The infrared & electro-optical systems handbook. Volume 7, Chapter 1. Bellingham, Washington: The International Society for Optical Engineering (SPIE), 1993. p 1–156. ISBN 0-8194-1072-1.
[19]	*Rafael Trophy active defence systems*. Jane's Armour and Artillery Upgrades, 2013. Posted: 14.11.2013. Found: https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1330133&Pubabbrev=JAAU

[20] *AN/AAR-44 infrared missile warning receiver*. C4ISR & Mission Systems: Air, 2013. Posted: 30.11.2013. Found: https://janes.ihs.com/CustomPages/Janes/DisplayPageaspx?DocType=Reference&ItemId=+++1525665&Pubabbrev=JC4IA

[21] *MWS-20 missile warning system*. Jane's Radar And Electronic Warfare Systems, 2013. Posted: 29.11.2013. Found: https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1380580&Pubabbrev=JREW

[22] *Saab EDS LWS-300/LWS-310 airborne laser warner*. Jane's Electro-Optic Systems, 2013. Posted: 17.1.2011. Found: https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1351092&Pubabbrev=JEOS

[23] *EN/ALR-400*. Jane's Radar And Electronic Warfare Systems, 2013. Post-ed: 29.11.2013. Found: https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1381178&Pubabbrev=JREW

[24] Stimson, George W: *Introduction to airborne radar*. El Segundo, CA: Hughes Aircraft Company, 1983. ix, 621 p.

[25] Kopp, Carlo: *Radar Warning Receivers and Defensive Electronic Countermeasures*. Australian Aviation, September 1998. [Referred: 13.4.2014] Found: http://www.ausairpower.net/TE-RWR-ECM.html

[26] *Integrated circuit*. Encyclopædia Britannica. [Referred: 13.4.2014] Found: http://global.britannica.com/EBchecked/topic/289645/integrated-circuit-IC

[27] *OR gate*. Wikipedia. Posted: 11.4.2014. [Referred: 13.4.2014] Found: http://en.wikipedia.org/wiki/OR_gate

[28] Richardson, M.A., et al: *Surveillance and Target Acquisition Systems*. 2nd ed. London UK: Brassey's, 1997. xii, 260 p. ISBN: 1 85753 137 X.

[29]	Quaranta, Paolo. *Electronic Warfare (EW) for Rotary Wing Platforms*. Military Technology, 2013 Vol. 37 Issue 4. p.52-55. ISSN: 0722-3226.
[30]	AN/APR-39(V) Radar Warning Receiver. Jane's Radar And Electronic Warfare Systems, 2013. Posted: 30.11.2013. Found: https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1339718&Pubabbrev=JAV_
[31]	*Chirp*. Wikipedia. Posted: 3.1.2014. [Referred: 13.4.2014.] Found: http://en.wikipedia.org/wiki/Chirp.
[32]	Klemola, Olli & Lehto, Arto. Tutkatekniikka.
[33]	Lesson 3: Jamming, Frequency controls, and electronic Deception. www.GlobalSecurity.org. Posted: 27.04.2005. [Referred: 13.4.2014] Found: http://www.globalsecurity.org/military/library/policy/army/accp/ss0134/lsn3.htm